internetsecuritysuite

Benutzerhandbuch

Version 8.0

McAfee®

COPYRIGHT

Copyright © 2005 McAfee, Inc. Alle Rechte vorbehalten. Kein Teil dieser Veröffentlichung darf ohne schriftliche Erlaubnis von McAfee, Inc., ihren Lieferanten oder zugehörigen Tochtergesellschaften in irgendeiner Form oder mit irgendwelchen Mitteln vervielfältigt, übertragen, transkribiert, in einem Informationsabrufsystem gespeichert oder in eine andere Sprache übersetzt werden.

MARKEN

ACTIVE FIREWALL, ACTIVE SECURITY, ACTIVESECURITY (UND IN KATAKANA), ACTIVESHIELD, ANTIVIRUS ANYWARE AND DESIGN, CLEAN-UP, DESIGN (STYLIZED E), DESIGN (STYLIZED N), ENTERCEPT, ENTERPRISE SECURECAST, ENTERPRISE SECURECAST (UND IN KATAKANA), EPOLICY ORCHESTRATOR, FIRST AID, FORCEFIELD, GMT, GROUPSHIELD, GROUPSHIELD (UND IN KATAKANA), GUARD DOG, HOMEGUARD, HUNTER, INTRUSHIELD, INTRUSION PREVENTION THROUGH INNOVATION, M AND DESIGN, MCAFEE, MCAFEE (UND IN KATAKANA), MCAFEE AND DESIGN, MCAFEE.COM, MCAFEE VIRUSSCAN, NA NETWORK ASSOCIATES, NET TOOLS, NET TOOLS (UND IN KATAKANA), NETCRYPTO, NETOCTOPUS, NETSCAN, NETSHIELD, NETWORK ASSOCIATES, NETWORK ASSOCIATES COLLISEUM, NETXRAY, NOTESGUARD, NUTS & BOLTS, OIL CHANGE, PC MEDIC, PCNOTARY, PRIMESUPPORT, RINGFENCE, ROUTER PM, SECURECAST, SECURESELECT, SPAMKILLER, STALKER, THREATSCAN, TIS, TMEG, TOTAL VIRUS DEFENSE, TRUSTED MAIL, UNINSTALLER, VIREX, VIRUS FORUM, VIRUSCAN, VIRUSSCAN, VIRUSSCAN (UND IN KATAKANA), WEBSCAN, WEBSHIELD, WEBSHIELD (UND IN KATAKANA), WEBSTALKER, WEBWALL, WHAT'S THE STATE OF YOUR IDS?, WHO'S WATCHING YOUR NETWORK, YOUR E-BUSINESS DEFENDER, YOUR NETWORK. OUR BUSINESS. sind eingetragene Marken oder Marken von McAfee, Inc. und/oder von ihren Tochterunternehmen in den USA und/oder anderen Ländern. Rot in Verbindung mit Sicherheit ist ein Wahrzeichen von McAfee-Markenprodukten. Alle anderen hier erwähnten eingetragenen und nicht eingetragenen Marken sind ausschließlich Eigentum ihrer jeweiligen Inhaber.

LIZENZINFORMATIONEN

Lizenzvertrag

HINWEIS FÜR ALLE BENUTZER: LESEN SIE DEN LIZENZVERTRAG FÜR DIE VON IHNEN ERWORBENE SOFTWARE SORGFÄLTIG DURCH. ER ENTHÄLT DIE ALLGEMEINEN BESTIMMUNGEN UND BEDINGUNGEN FÜR DIE VERWENDUNG DER LIZENZIERTEN SOFTWARE. WENN SIE NICHT WISSEN, WELCHEN SOFTWARE-LIZENZTYP SIE ERWORBEN HABEN, SCHLAGEN SIE IN DEN UNTERLAGEN ZUM KAUF UND WEITEREN UNTERLAGEN BEZÜGLICH DER LIZENZGEWÄHRUNG ODER DER BESTELLUNTERLAGEN NACH, DIE SIE ZUSAMMEN MIT DEM SOFTWAREPAKET ODER SEPARAT (ALS BROSCHÜRE, ALS DATEI AUF DER PRODUKT-CD ODER ALS DATEI AUF DER WEBSITE, VON DER SIE AUCH DAS SOFTWAREPAKET HERUNTERGELADEN HABEN) ERHALTEN HABEN. WENN SIE MIT DEN IN DIESEM VERTRAG AUFGEFÜHRTEN BESTIMMUNGEN NICHT EINVERSTANDEN SIND, DÜRFEN SIE DIE SOFTWARE NICHT INSTALLIEREN. FALLS ZUTREFFEND, KÖNNEN SIE DAS PRODUKT GEGEN RÜCKERSTATTUNG DES KAUFPREISES AN MCAFEE ODER AN DIE STELLE ZURÜCKGEBEN, AN DER SIE DAS PRODUKT ERWORBEN HABEN.

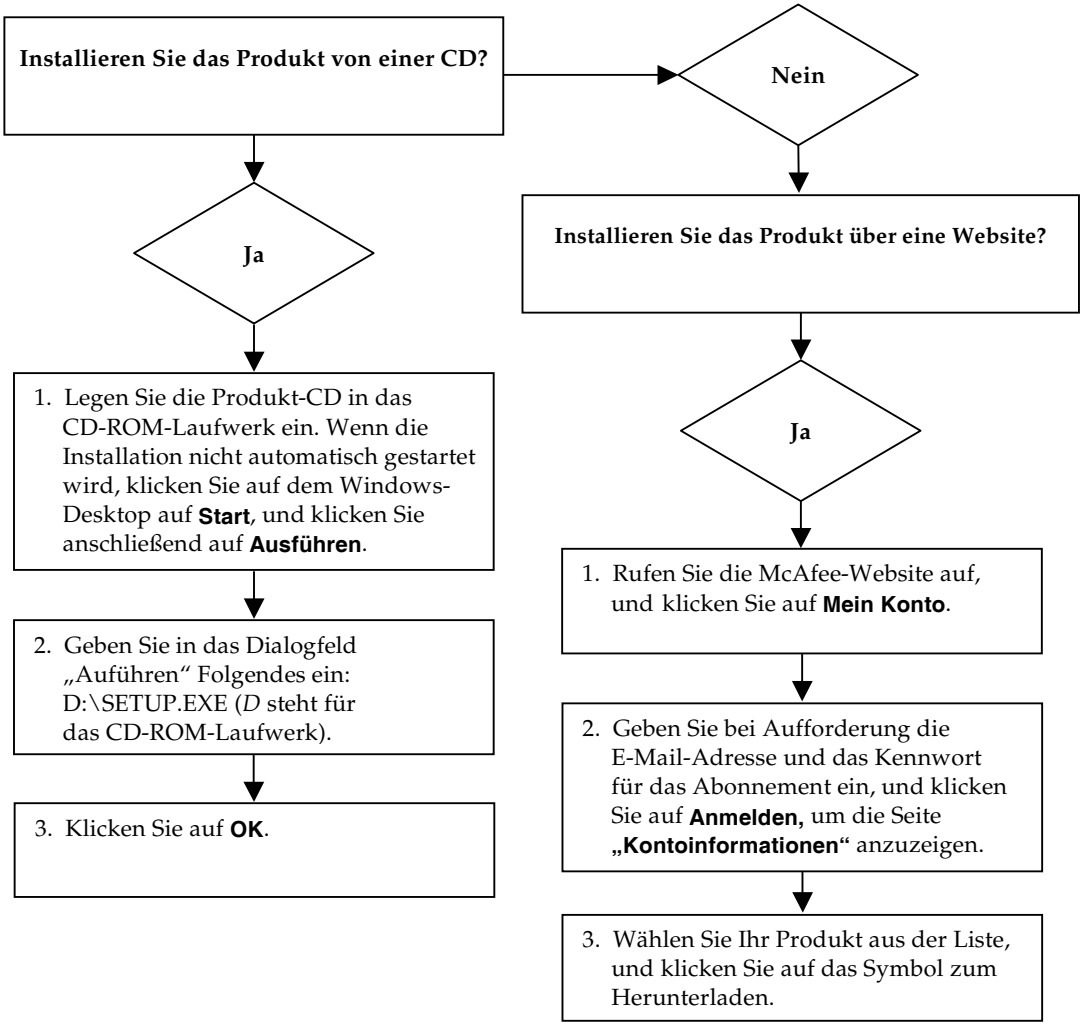
Zuweisungen

Im Lieferumfang dieses Produkts ist gegebenenfalls Folgendes enthalten:

♦ Software, die vom OpenSSL-Projekt zur Verwendung mit dem OpenSSL-Toolkit entwickelt wurde (http://www.openssl.org/). ♦ Kryptographie-Software, die von Eric Young entwickelt wurde, und Software, die von Tim J. Hudson entwickelt wurde. ♦ Softwareprogramme, die gemäß der GNU, General Public License (GPL) oder anderen ähnlichen Lizenzen für kostenlose Software zugelassen werden und es dem Benutzer neben anderen Rechten erlauben, bestimmte Programme oder Teile davon zu kopieren, zu modifizieren und weiterzugeben sowie auf den Quellcode zuzugreifen. Die GPL verlangt, dass grundsätzlich bei Weitergabe der Software an Dritte in einem ausführbaren binären Format im Geltungsbereich der GPL diesem Benutzer auch der Quellcode zur Verfügung gestellt werden muss. Bei Software dieser Art, die unter den Geltungsbereich der GPL fällt, wird der Quellcode ebenfalls auf der entsprechenden CD zur Verfügung gestellt. Falls Lizenzen für kostenlose Software verlangen, dass McAfee Rechte für die Nutzung, das Kopieren oder die Modifikation eines Softwareprogramms gewährt, die über die in diesem Vertrag gewährten Rechte hinausgehen, haben Rechte dieser Art Vorrang vor den Rechten und Einschränkungen in diesem Vertrag. ♦ Von Henry Spencer entwickelte Software, Copyright 1992, 1993, 1994, 1997 Henry Spencer. ♦ Von Robert Nordier entwickelte Software, Copyright © 1996-7 Robert Nordier. ♦ Von Douglas W. Sauder entwickelte Software. ♦ Von der Apache Software Foundation entwickelte Software (http://www.apache.org/). Eine Kopie des Lizenzvertrags für diese Software erhalten Sie unter www.apache.org/licenses/LICENSE-2.0.txt. ♦ International Components for Unicode („ICU"), Copyright © 1995-2002 International Business Machines Corporation und andere. ♦ Von CrystalClear Software, Inc. entwickelte Software, Copyright © 2000 CrystalClear Software, Inc. ♦ FEAD® Optimizer®-Technologie, Copyright Netopsystems AG, Berlin, Deutschland. ♦ Outside In® Viewer Technology, © 1992-2001 Stellent Chicago, Inc. und/oder Outside In® HTML Export, © 2001 Stellent Chicago, Inc. ♦ Software, urheberrechtlich geschützt von Thai Open Source Software Center Ltd. und Clark Cooper, © 1998, 1999, 2000. ♦ Software, urheberrechtlich geschützt von Expat maintainers. ♦ Software, urheberrechtlich geschützt von The Regents of the University of California, © 1989. ♦ Software, urheberrechtlich geschützt von Gunnar Ritter. ♦ Software, urheberrechtlich geschützt von Sun Microsystems®, Inc., © 2003. ♦ Software, urheberrechtlich geschützt von Gisle Aas, © 1995-2003. ♦ Software, urheberrechtlich geschützt von Michael A. Chase, © 1999-2000. ♦ Software, urheberrechtlich geschützt von Neil Winton, © 1995-1996. ♦ Software, urheberrechtlich geschützt von RSA Data Security, Inc., © 1990-1992. ♦ Software, urheberrechtlich geschützt von Sean M. Burke, © 1999, 2000. ♦ Software, urheberrechtlich geschützt von Martijn Koster, © 1995. ♦ Software, urheberrechtlich geschützt von Brad Appleton, © 1996-1999. ♦ Software, urheberrechtlich geschützt von Michael G. Schwern, © 2001. ♦ Software, urheberrechtlich geschützt von Graham Barr, © 1998. ♦ Software, urheberrechtlich geschützt von Larry Wall und Clark Cooper, © 1998-2000. ♦ Software, urheberrechtlich geschützt von Frodo Looijaard, © 1997. ♦ Software, urheberrechtlich geschützt von der Python Software Foundation, Copyright © 2001, 2002, 2003. Eine Kopie des Lizenzvertrags für diese Software erhalten Sie unter www.python.org. ♦ Software, urheberrechtlich geschützt von Beman Dawes, © 1994-1999, 2002. ♦ Software, geschrieben von Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek, © 1997-2000 University of Notre Dame. ♦ Software, urheberrechtlich geschützt von Simone Bordet & Marco Cravero, © 2002. ♦ Software, urheberrechtlich geschützt von Stephen Purcell, © 2001. ♦ Von Indiana University Extreme! Lab entwickelte Software (http://www.extreme.indiana.edu/). ♦ Software, urheberrechtlich geschützt von International Business Machines Corporation und anderen, © 1995-2003. ♦ Von der University of California, Berkeley und deren Mitwirkenden entwickelte Software. ♦ Von Ralf S. Engelschall, <rse@engelschall.com>, entwickelte Software für die Verwendung im mod_ssl-Projekt (http://www.modssl.org/). ♦ Software, urheberrechtlich geschützt von Kevlin Henney, © 2000-2002. ♦ Software, urheberrechtlich geschützt von Peter Dimov und Multi Media Ltd. © 2001, 2002. ♦ Software, urheberrechtlich geschützt von David Abrahams, © 2001, 2002. Dokumentation dazu finden Sie unter http://www.boost.org/libs/bind/bind.html. ♦ Software, urheberrechtlich geschützt von Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock, © 2000. ♦ Software, urheberrechtlich geschützt von Boost.org, © 1999-2002. ♦ Software, urheberrechtlich geschützt von Nicolai M. Josuttis, © 1999. ♦ Software, urheberrechtlich geschützt von Jeremy Siek, © 1999-2001. ♦ Software, urheberrechtlich geschützt von Daryle Walker, © 2001. ♦ Software, urheberrechtlich geschützt von Chuck Allison und Jeremy Siek, © 2001, 2002. ♦ Software, urheberrechtlich geschützt von Samuel Krempp, © 2001. Aktualisierungen, Dokumentation und Versionsverlauf dazu finden Sie unter http://www.boost.org. ♦ Software, urheberrechtlich geschützt von Doug Gregor (gregod@cs.rpi.edu), © 2001, 2002. ♦ Software, urheberrechtlich geschützt von Cadenza New Zealand Ltd., © 2000. ♦ Software, urheberrechtlich geschützt von Jens Maurer, © 2000, 2001. ♦ Software, urheberrechtlich geschützt von Jaakko Järvi (jaakko.jarvi@cs.utu.fi), © 1999, 2000. ♦ Software, urheberrechtlich geschützt von Ronald Garcia, © 2002. ♦ Software, urheberrechtlich geschützt von David Abrahams, Jeremy Siek und Daryle Walker, © 1999-2001. ♦ Software, urheberrechtlich geschützt von Stephen Cleary (shammah@voyager.net), © 2000. ♦ Software, urheberrechtlich geschützt von Housemarque Oy <http://www.housemarque.com>, © 2001. ♦ Software, urheberrechtlich geschützt von Paul Moore, © 1999. ♦ Software, urheberrechtlich geschützt von Dr. John Maddock, © 1998-2002. ♦ Software, urheberrechtlich geschützt von Greg Colvin und Beman Dawes, © 1998, 1999. ♦ Software, urheberrechtlich geschützt von Peter Dimov, © 2001, 2002. ♦ Software, urheberrechtlich geschützt von Jeremy Siek und John R. Bandela, © 2001. ♦ Software, urheberrechtlich geschützt von Joerg Walter und Mathias Koch, © 2000-2002.

Schnellreferenz

Wenn Sie die Installation des Produkts von einer CD oder Website ausführen, sollten Sie diese praktische Referenzseite ausdrucken.


Installieren Sie das Produkt von einer CD?
Nein
Ja
Installieren Sie das Produkt über eine Website?
Ja
1. Legen Sie die Produkt-CD in das CD-ROM-Laufwerk ein. Wenn die Installation nicht automatisch gestartet wird, klicken Sie auf dem Windows-Desktop auf Start, und klicken Sie anschließend auf Ausführen.
2. Geben Sie in das Dialogfeld „Auführen“ Folgendes ein: D:\SETUP.EXE (D steht für das CD-ROM-Laufwerk).
3. Klicken Sie auf OK.
1. Rufen Sie die McAfee-Website auf, und klicken Sie auf Mein Konto.
2. Geben Sie bei Aufforderung die E-Mail-Adresse und das Kennwort für das Abonnement ein, und klicken Sie auf Anmelden, um die Seite „Kontoinformationen“ anzuzeigen.
3. Wählen Sie Ihr Produkt aus der Liste, und klicken Sie auf das Symbol zum Herunterladen.

McAfee behält sich das Recht vor, Upgrade- und Support-Pläne sowie die entsprechenden Richtlinien jederzeit ohne Ankündigung zu ändern. McAfee und seine Produktnamen sind eingetragene Marken von McAfee, Inc. und/oder von seinen Tochterunternehmen in den USA und/oder anderen Ländern.
© 2005 McAfee, Inc. Alle Rechte vorbehalten.

Weitere Informationen

Zum Anzeigen der Benutzerhandbücher auf der Produkt-CD muss Acrobat Reader installiert sein. Andernfalls installieren Sie das Programm jetzt von der McAfee-Produkt-CD.

1. Legen Sie die Produkt-CD in das CD-ROM-Laufwerk ein.
2. Öffnen Sie Windows-Explorer: Klicken Sie auf dem Windows-Desktop auf **Start** und dann auf **Suchen**.
3. Suchen Sie den Ordner mit den Handbüchern (Manuals), und doppelklicken Sie auf die PDF-Datei des gewünschten Benutzerhandbuchs.

Registrierungsvorteile

McAfee empfiehlt, die im Produkt beschriebenen, einfachen Schritte zu befolgen, um Ihre Registrierung direkt an uns zu senden. Durch die Registrierung wird sichergestellt, dass Ihnen im angemessenen Zeitrahmen professionelle technische Unterstützung zur Verfügung steht. Außerdem profitieren Sie von:

- KOSTENLOSEM elektronischen Support
- Updates für Virusdefinitionsdateien (DAT-Dateien) für ein Jahr ab dem Zeitpunkt der Installation beim Kauf der VirusScan-Software

  Preisangaben für ein zusätzliches Jahr Virussignaturen erhalten Sie unter http://www.mcafee.com/.
- Garantie von 60 Tagen für Austausch der Software-CD, falls diese fehlerhaft oder beschädigt ist
- SpamKiller-Filter-Updates für ein Jahr ab dem Zeitpunkt der Installation beim Kauf der SpamKiller-Software

  Preisangaben für ein zusätzliches Jahr Filter-Updates erhalten Sie unter http://www.mcafee.com/.
- McAfee Internet Security Suite-Updates für ein Jahr ab dem Zeitpunkt der Installation beim Kauf der MIS-Software

  Preisangaben für ein zusätzliches Jahr Inhalts-Updates erhalten Sie unter http://www.mcafee.com/.

Technischer Support

Technischen Support erhalten Sie unter http://www.mcafeehilfe.com.

Unsere Support-Site ermöglicht Ihnen rund um die Uhr den Zugriff auf einen benutzerfreundlichen Antwort-Assistenten, der Ihnen Antworten auf die häufigsten Fragen gibt.

Die erweiterten Optionen sind für erfahrene Benutzer gedacht. Sie umfassen beispielsweise eine Schlüsselwortsuche und ein Hilfeverzeichnis. Wenn sich keine Lösung findet, können Sie außerdem KOSTENLOS auf unsere Dienste Chat Now! und E-Mail Express! zugreifen. Per Chat und E-Mail können Sie über das Internet schnell und kostenlos einen qualifizierten Support-Mitarbeiter erreichen. Sie können sich auch hier über die telefonischen Support-Möglichkeiten informieren: http://www.mcafeehilfe.com.

Inhalt

Schnellreferenz iii

1 Einführung 11

McAfee Internet Security-Software 12
Systemanforderungen 12
Verwenden von McAfee SecurityCenter 13
Deinstallieren von Internet Security Suite-Programmen 14

2 McAfee VirusScan 15

Neue Funktionen 15
Testen von VirusScan 16
Testen von ActiveShield 16
Testen von Scan 17
ActiveShield 18
Aktivieren bzw. Deaktivieren von ActiveShield 18
Konfigurieren von ActiveShield-Optionen 20
Übersicht über Sicherheitswarnungen 30
Manuelles Überprüfen des Computers 33
Manuelles Überprüfen auf Viren und andere Bedrohungen 33
Automatisches Überprüfen auf Viren und andere Bedrohungen 38
Übersicht über Bedrohungserkennungen 40
Verwalten von Dateien unter Quarantäne 41
Erstellen einer Rettungsdiskette 43
Einrichten des Schreibschutzes für eine Rettungsdiskette 44
Verwenden einer Rettungsdiskette 45
Aktualisieren einer Rettungsdiskette 45
Automatisches Melden von Viren 45
Weiterleiten von Informationen an die World Virus Map 45
Anzeigen der World Virus Map 46
Aktualisieren von VirusScan 47
Automatisches Prüfen auf Updates 48
Manuelles Prüfen auf Updates 48

3 McAfee Personal Firewall Plus 51

Neue Funktionen 51
Entfernen anderer Firewalls 53
Festlegen der Standard-Firewall 53
Festlegen der Sicherheitsstufe 54
Testen von McAfee Personal Firewall Plus 57
Info zur Zusammenfassung 57
Info zur Seite „Internetanwendungen“ 63
Ändern von Anwendungsregeln 64
Zulassen und Blockieren von Internetanwendungen 64
Info zur Seite Eingehende Ereignisse 65
Erläuterungen zu Ereignissen 66
Anzeigen von Ereignissen im Ereignisprotokoll 68
Reagieren auf eingehende Ereignisse 71
Verwalten des Protokolls eingehender Ereignisse 75
Info zu Warnungen 77
Rote Warnungen 77
Grüne Warnungen 83
Blaue Warnungen 84

4 McAfee Privacy Service 87

Funktionen 87
Der Administrator 87
Setup-Assistent 88
Wiederbeschaffen des Administratorkennworts 88
Der Startbenutzer 89
Öffnen von McAfee Privacy Service 89
Öffnen von und Anmelden bei Privacy Service 89
Deaktivieren von Privacy Service 89
Aktualisieren von McAfee Privacy Service 90
Benutzer hinzufügen 90
Festlegen des Kennworts 90
Festlegen der Altersgruppe 90
Festlegen des Cookie Blocker 91
Festlegen der Internetzugriffszeiten 91
Bearbeiten von Benutzern 92
Ändern von Kennwörtern 92

Ändern der Informationen eines Benutzers 92
Ändern der Cookie Blocker-Einstellung 93
Bearbeiten der Liste für akzeptierte und abgelehnte Cookies 93
Ändern der Altersgruppe 94
Ändern der Internetzugriffszeiten 94
Ändern des Startbenutzers 95
Entfernen von Benutzern 95
Optionen 95
Blockieren von Websites 95
Zulassen von Websites 96
Blockieren von Informationen 96
Hinzufügen von Informationen 96
Bearbeiten von Informationen 97
Entfernen persönlicher Daten 97
Blockieren von Web-Bugs 97
Blockieren von Werbung 97
Zulassen von Cookies von bestimmten Websites 98
Ereignisprotokoll 98
Datum und Uhrzeit 98
Benutzer 99
Zusammenfassung 99
Ereignisdetails 99
Speichern des aktuellen Protokolls 99
Anzeigen von gespeicherten Protokollen 99
Dienstprogramme 100
Dauerhaftes Löschen von Dateien mithilfe von McAfee Shredder 100
Warum Windows Dateireste zurücklässt 100
Was McAfee Shredder löscht 100
Dauerhaftes Löschen von Dateien in Windows-Explorer 101
Leeren des Papierkorbs unter Windows 101
Anpassen der Shredder-Einstellungen 101
Sichern der Privacy Service-Datenbank 101
Wiederherstellen der Sicherungsdatenbank 102
Benutzeroptionen 103
Ändern Ihres Kennworts 103
Ändern Ihres Benutzernamens 103
Leeren des Cache 104

Akzeptieren von Cookies 104
Gehen Sie wie folgt vor, wenn Sie eine Website aus dieser Liste entfernen müssen: 104
Ablehnen von Cookies 105
Gehen Sie wie folgt vor, wenn Sie eine Website aus dieser Liste entfernen müssen: 105

5 McAfee SpamKiller 107

Funktionen 107
Benutzeroptionen 108
Filtern 108
Erläuterungen zur Symbolleiste 108
Deaktivieren von SpamKiller 109
Erläuterungen zur Seite „Zusammenfassung“ 110
Integration in Microsoft Outlook und Outlook Express 111
Verwalten von E-Mail-Konten und Benutzern 111
Hinzufügen von E-Mail-Konten 111
Einrichten von E-Mail-Clients für die Verwendung von SpamKiller 112
Löschen von E-Mail-Konten 112
Löschen eines E-Mail-Kontos aus SpamKiller 113
Bearbeiten der Eigenschaften von E-Mail-Konten 113
POP3-Konten 113
MSN/Hotmail-Konten 115
MAPI-Konten 117
Hinzufügen von Benutzern 119
Benutzerkennwörter und Kinderschutz vor Spam 120
Anmelden bei SpamKiller auf einem Computer mit mehreren Benutzern 122
Verwenden der Freunde-Liste 123
Öffnen einer Freunde-Liste 124
Importieren von Adressbüchern 124
Automatisches Importieren von Adressbüchern 125
Manuelles Importieren von Adressbüchern 125
Bearbeiten von Adressbuchinformationen 126
Löschen von Adressbüchern aus der Liste der automatisch importierten Adressbücher 126
Hinzufügen von Freunden 127
Hinzufügen von Freunden über die Registerkarte „Blockierte E-Mails“ oder „Akzeptierte E-Mails“ 127
Hinzufügen von Freunden über die Seite „Freunde“ 128
Hinzufügen von Freunden über Microsoft Outlook: 128

Bearbeiten von Einträgen in den Freunde-Listen 129
Löschen von Freunde-Einträgen 129
Arbeiten mit blockierten und akzeptierten Nachrichten 130
Registerkarte „Blockierte E-Mails“ 130
Registerkarte „Akzeptierte E-Mails“ 132
Aufgaben für blockierte und akzeptierte E-Mails 133
Wiederherstellen von Nachrichten 134
Über die Registerkarte „Blockierte E-Mails“ 134
Über den SpamKiller-Ordner in Microsoft Outlook oder Outlook Express 134
Blockieren von Nachrichten 134
Über die Registerkarte „Akzeptierte E-Mails“ 135
Über Microsoft Outlook 135
Speicherort der blockierten Nachrichten 135
Manuelles Löschen von Nachrichten 135
Ändern der Einstellungen, wie Spam-Nachrichten behandelt werden 136
Markieren mit Tags 136
Blockieren 136
Ändern der Einstellungen, wie Spam-Nachrichten von SpamKiller behandelt werden 136
Verwenden des Anti-Phishing-Filters 137
Hinzufügen von Freunden zu einer Freunde-Liste 137
Hinzufügen von Filtern 138
Regelmäßige Ausdrücke 140
Melden von Spam-Nachrichten an McAfee 143
Manuelles Senden von Beschwerden 143
Senden von Fehlermeldungen 144
Manuelles Senden von Fehlermeldungen 144

Index 145

Einführung 1

Das Internet bietet direkten Zugriff auf eine Fülle von Informationen und jede Menge Unterhaltung. Sobald Sie jedoch eine Verbindung zum Internet herstellen, ist Ihr Computer zahlreichen Sicherheitsbedrohungen ausgesetzt. Schützen Sie Ihre Privatsphäre, und sichern Sie Ihren Computer und Ihre Daten mit McAfee Internet Security Suite. Unter Einsatz der mehrfach ausgezeichneten Technologien von McAfee bietet Internet Security Suite eine der umfangreichsten Zusammenstellungen von Tools für Datenschutz und Sicherheit, die zurzeit erhältlich sind. Mit McAfee Internet Security Suite können Sie Viren zerstören, Hacker überlisten, Ihre persönlichen Daten schützen, Ihre Aufenthalte im Web persönlicher gestalten sowie Werbung und Popup-Fenster blockieren. Sie haben die Möglichkeit, Cookies und Kennwörter zu verwalten, Dateien, Ordner und Laufwerke zu sperren, anstößige Inhalte zu filtern und die Eingangs- und Ausgangsverbindungen Ihres Computers mit dem Internet zu steuern.

McAfee Internet Security ist eine bewährte Sicherheitslösung, die Internetbenutzern von heute einen leistungsstarken Schutz bietet.

McAfee Internet Security Suite umfasst die folgenden Produkte:

- *McAfee VirusScan* auf Seite 15
- *McAfee Personal Firewall Plus* auf Seite 51
- *McAfee Privacy Service* auf Seite 87
- *McAfee SpamKiller* auf Seite 107

McAfee Internet Security-Software

- **McAfee SecurityCenter:** Beurteilt die Sicherheitsrisiken für Ihren PC, und Sie werden entsprechend informiert und gewarnt. Jeder Sicherheitsindex schätzt Ihr Risiko hinsichtlich Sicherheit und internetbasierter Bedrohungen schnell ein und empfiehlt rasche und sichere Schutzmaßnahmen für Ihren Computer.
- **McAfee VirusScan:** Führt einen Scan durch und erkennt, repariert und entfernt Internetviren. Sie können Virenüberprüfungen anpassen und die Reaktion und Maßnahme festlegen, die bei der Erkennung eines Virus erfolgen sollen. Sie können VirusScan auch so konfigurieren, dass alle auf Ihrem Computer ausgeführten, virenbezogenen Aktionen aufgezeichnet werden.
- **McAfee Personal Firewall Plus:** Schützt Ihren Computer, während er mit dem Internet verbunden ist, und sichert die Eingangs- und Ausgangsverbindungen Ihres Computers mit dem Internet.
- **McAfee Privacy Service:** Vereint den Schutz persönlicher Daten mit dem Blockieren von Werbung sowie modernster Filtertechnologie. Sichert Ihre persönlichen Daten und bietet gleichzeitig größere Kontrolle über das Surfverhalten Ihrer Familie im Internet. Der McAfee Privacy Service gewährleistet, dass keine vertraulichen Informationen gegenüber Online-Gefahren zugänglich gemacht werden, und schützt Sie und Ihre Familie somit vor unerwünschten Inhalten aus dem Internet.
- **McAfee SpamKiller:** Bei der zunehmenden Zahl betrügerischer, unerwünschter und beleidigender E-Mails an Erwachsene, Kinder und Unternehmen ist ein Schutz vor Spam-Mails ein wesentlicher Bestandteil der Sicherheitsstrategie für Ihren Computer.

Systemanforderungen

- Microsoft® Windows 98, Me, 2000 oder XP
- PC mit Pentium-kompatiblem Prozessor
  - Windows 98, 2000: 133 MHz oder höher
  - Windows Me: 150 MHz oder höher
  - Windows XP (Home und Professional): 300 MHz oder höher
- RAM
  - Windows 98, Me, 2000: 64 MB
  - Windows XP (Home und Professional): 128 MB
- 100 MB Festplattenspeicher
- Microsoft® Internet Explorer ab Version 5.5

HINWEIS: Sie können die neueste Version von Internet Explorer von der Microsoft-Website unter http://www.microsoft.com/ **herunterladen.**

Verwenden von McAfee SecurityCenter

Das McAfee SecurityCenter stellt Ihre Anlaufstelle für alle Sicherheitsbelange dar und ist über das Symbol auf der Windows-Taskleiste oder dem Windows-Desktop zugänglich. Mit diesem Programm können Sie auf folgende nützliche Dienste zugreifen:

- Kostenlose Sicherheitsanalyse für Ihren Computer.
- Starten, Verwalten und Konfigurieren aller McAfee-Abonnements über ein einziges Symbol.
- Anzeige fortwährend aktualisierter Viruswarnungen und der neuesten Produktinformationen.
- Direkte Links zu häufig gestellten Fragen und Antworten sowie Kontoinformationen auf der McAfee-Website.

> **HINWEIS**
> Weitere Informationen zu SecurityCenter-Funktionen erhalten Sie, wenn Sie im Dialogfeld **SecurityCenter** auf **Hilfe** klicken.

Wenn SecurityCenter ausgeführt wird und alle auf Ihrem Computer installierten McAfee-Funktionen aktiviert sind, wird das Symbol mit dem roten **M** auf der Windows-Taskleiste angezeigt. Dieser Bereich, der auch die Systemuhr enthält, befindet sich in der Regel unten rechts auf dem Windows-Desktop.

Wenn auf Ihrem Computer installierte McAfee-Anwendungen deaktiviert sind, wird das McAfee-Symbol schwarz dargestellt .

So öffnen Sie McAfee SecurityCenter:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste.
2. Klicken Sie auf **SecurityCenter öffnen**.

So greifen Sie auf Ihr McAfee-Produkt zu:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste.
2. Zeigen Sie auf das entsprechende McAfee-Produkt, und klicken Sie dann auf die zu verwendende Funktion.

Deinstallieren von Internet Security Suite-Programmen

In manchen Fällen möchten Sie Internet Security Suite oder einige seiner zugehörigen Programme möglicherweise entfernen.

HINWEIS
Zum Deinstallieren von Internet Security Suite benötigen Sie Administratorrechte.

1. Speichern Sie Ihre Arbeit, und schließen Sie alle geöffneten Anwendungen.
2. Öffnen Sie die **Systemsteuerung**.
   - Wählen Sie in der Windows-Taskleiste **Start**, zeigen Sie auf **Einstellungen**, und klicken Sie auf **Systemsteuerung** (Windows 98, ME und 2000).
   - Wählen Sie in der Windows-Taskleiste **Start**, und klicken Sie anschließend auf **Systemsteuerung** (Windows XP).
3. Klicken Sie auf **Software**.
4. Wählen Sie den Deinstallations-Assistenten für McAfee und anschließend ein oder mehr Programme aus, und klicken Sie auf **Deinstallieren**.
5. Klicken Sie auf **Ja**, um mit dem Entfernen fortzufahren.
6. Starten Sie Ihren Computer neu, wenn Sie dazu aufgefordert werden.

McAfee VirusScan 2

Willkommen bei McAfee VirusScan.

McAfee VirusScan ist ein Anti-Virus-Abonnementservice, der Ihnen umfassenden, zuverlässigen und stets aktuellen Virenschutz bietet. Unterstützt durch die preisgekrönte McAfee-Scan-Technologie schützt VirusScan vor Viren, Würmern, Trojanern, bösartigen Skripts und Hybridangriffen.

Das Programm umfasst folgende Funktionen:

ActiveShield: ActiveShield durchsucht alle Dateien, auf die Sie oder Ihr Computer zugreifen.

Scan: Durchsucht Festplatten, Disketten sowie einzelne Dateien und Ordner nach Viren und möglicherweise unerwünschten Programmen.

Quarantäne: Verschlüsselt infizierte bzw. verdächtige Dateien und isoliert sie temporär in einem Ordner, bis eine angemessene Maßnahme ergriffen werden kann.

Erkennung feindseliger Aktivitäten: Überwacht den Computer auf virenähnliche Aktivitäten, die durch Würmer und bösartige Skripts verursacht werden.

Neue Funktionen

Diese Version von VirusScan enthält folgende neue Funktionen:

- **Erkennung und Entfernung von Spyware und Adware**
  VirusScan identifiziert und entfernt Spyware, Adware und andere Programme, die Ihre Privatsphäre verletzen und die Leistung Ihres Computers beeinträchtigen.
- **Tägliche automatische Updates**
  Tägliche automatische VirusScan-Updates schützen Sie vor den neuesten identifizierten und nicht identifizierten Computerbedrohungen.
- **Schnelles Scannen im Hintergrund**
  Schnelle, im Hintergrund ausgeführte Scans identifizieren und zerstören Viren, trojanische Pferde, Spyware, Adware, Dialer und andere bösartige Programme, ohne Sie bei der Arbeit zu unterbrechen.
- **Echtzeit-Sicherheitswarnungen**
  Sicherheitswarnungen benachrichtigen Sie über den Ausbruch neuer Viren und Sicherheitsbedrohungen. Sie bieten auch Reaktionsoptionen zum Entfernen und Neutralisieren der Bedrohung und enthalten weitere Informationen dazu.

- **Erkennung und Bereinigung an mehreren Eintrittspunkten**
  VirusScan führt die Überwachung und Bereinigung an den Haupteintrittspunkten des Computers durch: E-Mail, Anlagen von Instant Messages und Internetdownloads.
- **Überwachung von E-Mails auf wurmähnliche Aktivitäten**
  WormStopper™ überwacht den Computer auf verdächtiges Massen-Mail-Verhalten und verhindert, dass sich Viren und Würmer per E-Mail auf andere Computer ausbreiten.
- **Überwachung von Skripts auf wurmähnliche Aktivitäten**
  ScriptStopper™ überwacht den Computer auf verdächtige Skriptausführungen und verhindert, dass sich Viren und Würmer per E-Mail auf andere Computer ausbreiten.
- **Kostenloser technischer Support per Instant Messaging und E-Mail**
  Der live bereitgestellte technische Support bietet leicht zugängliche und schnelle Beratung mithilfe von Instant Messaging und E-Mail.

Testen von VirusScan

Bevor Sie VirusScan zum ersten Mal verwenden, sollten Sie Ihre Installation testen. Gehen Sie für das separate Testen der ActiveShield- und Scan-Funktionen wie nachfolgend beschrieben vor.

Testen von ActiveShield

HINWEIS
Zum Testen von ActiveShield über die Registerkarte **VirusScan** klicken Sie in SecurityCenter auf VirusScan testen, um online Fragen und Antworten mit den folgenden Schritten anzuzeigen.

So testen Sie ActiveShield:

1. Rufen Sie http://www.eicar.com/ in Ihrem Webbrowser auf.
2. Klicken Sie auf den Link **The AntiVirus testfile eicar.com**.
3. Führen Sie einen Bildlauf zum unteren Ende der Seite durch. Unter **Download** werden vier Links angezeigt.
4. Klicken Sie auf **eicar.com**.

Wenn ActiveShield korrekt ausgeführt wird, wird die Datei eicar.com sofort nach Klicken auf den Link als Virus erkannt. Wenn Sie sehen möchten, wie VirusScan mit Viren umgeht, versuchen Sie, infizierte Dateien zu löschen oder unter Quarantäne zu stellen. Nähere Informationen dazu finden Sie unter *Übersicht über Sicherheitswarnungen* auf Seite 30.

Testen von Scan

Bevor Sie Scan testen können, müssen Sie ActiveShield deaktivieren, um zu verhindern, dass infizierte Dateien von ActiveShield erkannt werden, bevor Scan sie erkennt, und anschließend die Testdateien herunterladen.

So laden Sie die Testdateien herunter:

1. Deaktivieren Sie ActiveShield: Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Deaktivieren**.
2. Laden Sie die EICAR-Testdateien von der EICAR-Website herunter:
   a. Rufen Sie http://www.eicar.com/ auf.
   b. Klicken Sie auf den Link **The AntiVirus testfile eicar.com**.
   c. Führen Sie einen Bildlauf zum unteren Ende der Seite durch. Unter **Download** werden diese Links angezeigt:

      eicar.com enthält eine Textzeile, die von VirusScan als Virus erkannt wird.

      eicar.com.txt (optional) ist dieselbe Datei, jedoch mit einem anderen Dateinamen. Diese Datei ist für diejenigen Benutzer vorgesehen, die mit dem ersten Link Probleme haben. Benennen Sie die Datei nach dem Download einfach in „eicar.com“ um.

      eicar_com.zip ist eine Kopie des Testvirus in einer mit WinZip™ komprimierten ZIP-Datei (ein WinZip-Dateiarchiv).

      eicarcom2.zip ist eine Kopie des Testvirus in einer mit WinZip komprimierten ZIP-Datei, die sich ebenfalls in einer mit WinZip komprimierten ZIP-Datei befindet.

   d. Klicken Sie auf den jeweiligen Link, um die entsprechende Datei herunterzuladen. Für jede Datei wird ein Dialogfeld für den **Dateidownload** geöffnet.
   e. Klicken Sie auf **Speichern** und auf die Schaltfläche **Neuen Ordner erstellen**, und benennen Sie den Ordner anschließend in **VSO-Scan-Ordner** um.
   f. Doppelklicken Sie in jedem Dialogfeld **Speichern unter** auf **VSO-Scan-Ordner** und dann erneut auf **Speichern**.
3. Wenn Sie die Dateien heruntergeladen haben, schließen Sie Internet Explorer.
4. Aktivieren Sie ActiveShield: Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Aktivieren**.

So testen Sie Scan:

1 Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Auf Viren überprüfen**.

2 Navigieren Sie über die Verzeichnisstruktur im linken Bereich des Dialogfeldes zum **VSO-Scan-Ordner**, in dem Sie die Dateien gespeichert haben:

   a Klicken Sie auf das Pluszeichen (**+**) neben dem Laufwerkbuchstaben C.

   b Klicken Sie auf den **VSO-Scan-Ordner**, um ihn zu markieren (und nicht auf das**+** Pluszeichen neben dem Ordner).

   Dadurch wird Scan angewiesen, nur diesen Ordner nach Viren zu durchsuchen. Eine noch überzeugendere Demonstration der Fähigkeiten von Scan erhalten Sie, wenn Sie die Dateien an zufällig ausgewählten Standorten auf der Festplatte speichern.

3 Vergewissern Sie sich im Bereich **Prüfoptionen** des Dialogfeldes **Auf Viren überprüfen**, dass alle Optionen aktiviert sind.

4 Klicken Sie unten rechts im Dialogfeld auf **Scan**.

   VirusScan durchsucht den **VSO-Scan-Ordner**. Die EICAR-Testdateien, die Sie in diesem Ordner gespeichert haben, werden in der **Liste der erkannten Dateien** aufgeführt. In diesem Fall arbeitet Scan korrekt.

Wenn Sie sehen möchten, wie Scan mit Viren umgeht, versuchen Sie, infizierte Dateien zu löschen oder unter Quarantäne zu stellen. Nähere Informationen dazu finden Sie unter *Übersicht über Bedrohungserkennungen* auf Seite 40.

ActiveShield

Nachdem ActiveShield gestartet (in den Computerspeicher geladen) und aktiviert wurde, bietet das Programm konstanten Schutz für Ihren Computer. ActiveShield durchsucht alle Dateien, auf die Sie oder Ihr Computer zugreifen. Sollte ActiveShield eine infizierte Datei entdecken, wird automatisch versucht, den Virus zu bereinigen. Wenn ActiveShield den Virus nicht bereinigen kann, können Sie die Datei unter Quarantäne stellen oder löschen.

Aktivieren bzw. Deaktivieren von ActiveShield

ActiveShield wird standardmäßig gestartet (in den Computerspeicher geladen) und aktiviert (gekennzeichnet durch das rote Symbol auf der Windows-Taskleiste), sobald Sie Ihren Computer nach erfolgreicher Installation neu starten.

Wenn ActiveShield angehalten (nicht geladen) oder deaktiviert wird (gekennzeichnet durch das schwarze Symbol), können Sie das Programm manuell starten. Sie können ActiveShield auch so konfigurieren, dass das Programm automatisch nach jedem Start von Windows ausgeführt wird.

Aktivieren von ActiveShield

So aktivieren Sie ActiveShield für die aktuelle Windows-Sitzung:

Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Aktivieren**. Das McAfee-Symbol wird rot dargestellt .

Wenn ActiveShield weiterhin so konfiguriert ist, dass das Programm bei jedem Neustart von Windows ausgeführt wird, werden Sie in einer Meldung darüber informiert, dass Ihr Computer jetzt vor Viren geschützt ist. Andernfalls wird ein Dialogfeld geöffnet, in dem Sie ActiveShield so konfigurieren können, dass das Programm nach jedem Neustart von Windows ausgeführt wird (Abbildung 2-1 auf Seite 20).

Deaktivieren von ActiveShield

So deaktivieren Sie ActiveShield für die aktuelle Windows-Sitzung:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Deaktivieren**.
2. Klicken Sie auf **Ja**, um den Vorgang zu bestätigen.

   Das McAfee-Symbol wird schwarz dargestellt .

Wenn ActiveShield so konfiguriert ist, dass das Programm beim Start von Windows automatisch ausgeführt wird, ist Ihr Computer nach einem Neustart wieder vor Viren geschützt.

Konfigurieren von ActiveShield-Optionen

Sie können die Start- und Scan-Optionen von ActiveShield ändern. Verwenden Sie hierzu im Dialogfeld mit den **VirusScan-Optionen** (Abbildung 2-1) die Registerkarte **ActiveShield**. Der Zugriff erfolgt über das McAfee-Symbol auf der Windows-Taskleiste.

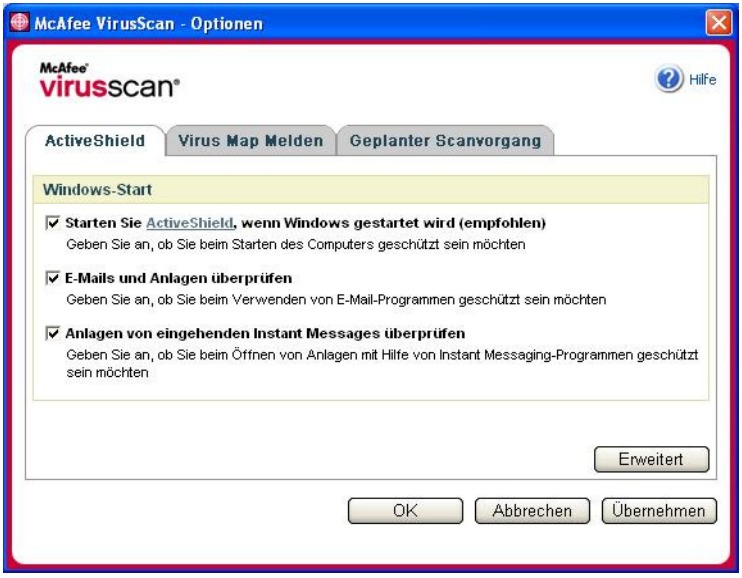

McAfee VirusScan - Optionen
McAfee
virusscan
Hilfe
ActiveShield
Virus Map Melden
Geplanter Scanvorgang
Windows-Start
Starten Sie ActiveShield, wenn Windows gestartet wird (empfohlen)
Geben Sie an, ob Sie beim Starten des Computers geschützt sein möchten
E-Mails und Anlagen überprüfen
Geben Sie an, ob Sie beim Verwenden von E-Mail-Programmen geschützt sein möchten
Anlagen von eingehenden Instant Messages überprüfen
Geben Sie an, ob Sie beim Öffnen von Anlagen mit Hilfe von Instant Messaging-Programmen geschützt sein möchten
Erweitert
OK
Abbrechen
Übernehmen

Abbildung 2-1. ActiveShield-Optionen

Starten von ActiveShield

ActiveShield wird standardmäßig gestartet (in den Computerspeicher geladen) und aktiviert (gekennzeichnet durch das rote Symbol), sobald Sie Ihren Computer nach erfolgreicher Installation neu starten.

Wenn ActiveShield angehalten ist (gekennzeichnet durch das schwarze Symbol), können Sie das Programm so konfigurieren, dass es nach jedem Start von Windows automatisch ausgeführt wird (empfohlen).

HINWEIS

Während der Installation von VirusScan-Updates kann der **Update-Assistent** ActiveShield ggf. vorübergehend beenden, um neue Dateien zu installieren. Wenn Sie vom **Update-Assistenten** aufgefordert werden, auf **Fertig stellen** zu klicken, wird ActiveShield erneut gestartet.

So starten Sie ActiveShield automatisch beim Start von Windows:

1 Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Optionen**.

Das Dialogfeld **VirusScan-Optionen** wird geöffnet (Abbildung 2-1 auf Seite 20).

2 Aktivieren Sie das Kontrollkästchen **ActiveShield ausführen, wenn Windows gestartet wird (empfohlen)**, und klicken Sie auf **Übernehmen**, um Ihre Änderungen zu speichern.

3 Klicken Sie zur Bestätigung auf **OK** und anschließend erneut auf **OK**.

Anhalten von ActiveShield

WARNUNG
Mit dem Anhalten von ActiveShield verliert Ihr Computer den Virenschutz. Wenn Sie ActiveShield zu anderen Zwecken als zur Aktualisierung anhalten müssen, vergewissern Sie sich, dass keine Verbindung mit dem Internet besteht.

So verhindern Sie die automatische Ausführung von ActiveShield beim Start von Windows:

1 Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Optionen**.

Das Dialogfeld **VirusScan-Optionen** wird geöffnet (Abbildung 2-1 auf Seite 20).

2 Deaktivieren Sie das Kontrollkästchen **ActiveShield ausführen, wenn Windows gestartet wird (empfohlen)**, und klicken Sie auf **Übernehmen**, um Ihre Änderungen zu speichern.

3 Klicken Sie zur Bestätigung auf **OK** und anschließend erneut auf **OK**.

Prüfen von E-Mails und Anlagen

Standardmäßig werden die Überprüfung von E-Mails und die automatische Bereinigung über die Option **E-Mails und Anlagen überprüfen** (Abbildung 2-1 auf Seite 20) aktiviert.

Wenn diese Option aktiviert ist, führt ActiveShield automatisch die Virenprüfung durch und versucht, eingehende (POP3) und ausgehende (SMTP) infizierte E-Mail-Nachrichten und Anlagen für den Großteil gängiger E-Mail-Clients zu reinigen. Hierzu zählen:

- Microsoft Outlook Express ab Version 4.0
- Microsoft Outlook ab Version 97
- Netscape Messenger ab Version 4.0
- Netscape Mail ab Version 6.0

- Eudora Light ab Version 3.0
- Eudora Pro ab Version 4.0
- Eudora ab Version 5.0
- Pegasus ab Version 4.0

HINWEIS
Für folgende E-Mail-Clients wird der E-Mail-Scan nicht unterstützt: Webbasierte E-Mail-Clients, IMAP, AOL, POP3 SSL und Lotus Notes. E-Mail-Anlagen werden jedoch beim Öffnen von ActiveShield geprüft.

Wenn Sie die Option **E-Mails und Anlagen überprüfen** deaktivieren, werden die E-Mail-Scan-Optionen und die WormStopper-Optionen (Abbildung 2-2 auf Seite 23) automatisch deaktiviert. Bei Deaktivierung der Prüfung ausgehender E-Mails werden die WormStopper-Optionen ebenfalls automatisch deaktiviert.

Wenn Sie Ihre E-Mail-Scan-Optionen ändern, müssen Sie anschließend das E-Mail-Programm neu starten, um die Änderungen in Kraft zu setzen.

Eingehende E-Mails

Wenn eine eingehende E-Mail-Nachricht oder Anlage infiziert ist, führt ActiveShield folgende Schritte durch:

- Es wird versucht, die infizierte E-Mail zu bereinigen.
- Es wird versucht, E-Mails, die nicht bereinigt werden können, unter Quarantäne zu stellen oder zu löschen.
- Es wird eine Warnungsdatei in die eingehende E-Mail aufgenommen, die Informationen zu den Schritten enthält, die zur Beseitigung der Infektion durchgeführt wurden.

Ausgehende E-Mails

Wenn eine ausgehende E-Mail-Nachricht oder Anlage infiziert ist, führt ActiveShield folgende Schritte durch:

- Es wird versucht, die infizierte E-Mail zu bereinigen.
- Es wird versucht, E-Mails, die nicht bereinigt werden können, unter Quarantäne zu stellen oder zu löschen.

HINWEIS
Einzelheiten zu Fehlermeldungen bei der Prüfung ausgehender E-Mails finden Sie in der Online-Hilfe.

Deaktivieren der Prüfung von E-Mails

Standardmäßig prüft ActiveShield sowohl eingehende als auch ausgehende E-Mails. Bei Bedarf können Sie jedoch festlegen, dass nur die eingehende oder nur die ausgehende E-Mail von ActiveShield geprüft wird.

So deaktivieren Sie die Prüfung der eingehenden bzw. ausgehenden E-Mail:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Erweitert**, und aktivieren Sie dann die Registerkarte **E-Mail-Scan** (Abbildung 2-2).
3. Deaktivieren Sie das Kontrollkästchen **Eingehende E-Mail-Nachrichten** oder **Ausgehende E-Mail-Nachrichten**, und klicken Sie auf **OK**.

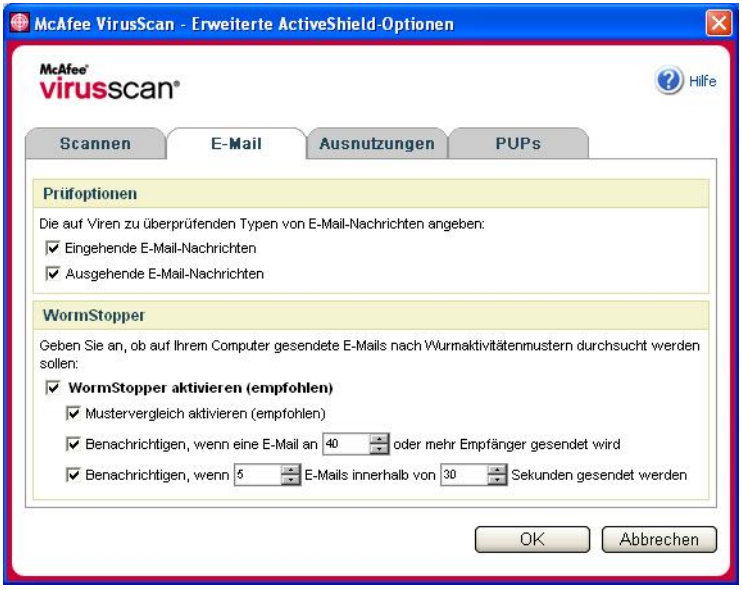


Abbildung 2-2. Erweiterte ActiveShield-Optionen - Registerkarte „E-Mail“

Prüfen auf Würmer

VirusScan überwacht den Computer auf verdächtige Aktivitäten, die möglicherweise darauf hinweisen, dass Ihr Computer akut gefährdet ist. Durch VirusScan werden Viren bereinigt, durch WormStopper™ hingegen wird der weiteren Verbreitung von Viren und Würmern vorgebeugt.

Computerwürmer sind sich selbst replizierende Viren, die sich im Arbeitsspeicher eines Computers befinden und Kopien von sich selbst per E-Mail verbreiten. Ohne WormStopper bemerken Sie Würmer unter Umständen erst, wenn durch ihr unkontrolliertes Fortpflanzen Systemressourcen belegt und dadurch die Leistung beeinträchtigt oder Tasks angehalten werden.

Durch den WormStopper-Schutzmechanismus werden bösartige Aktivitäten erkannt, gemeldet und blockiert. Zu verdächtigen Aktivitäten auf dem Computer zählt Folgendes:

- Ein Versuch, eine E-Mail an einen Großteil der Adressen in Ihrem Adressbuch weiterzuleiten
- Versuche, mehrere E-Mail-Nachrichten in schneller Folge weiterzuleiten

Wenn Sie ActiveShield so einstellen, dass die Standardoption **WormStopper aktivieren (empfohlen)** im Dialogfeld **Erweiterte Optionen** verwendet wird, überwacht WormStopper die E-Mail-Aktivität auf verdächtige Muster und gibt eine Warnung aus, wenn eine festgelegte Anzahl an E-Mails oder Empfängern innerhalb eines festgelegten Intervalls überschritten wird.

So konfigurieren Sie ActiveShield zur Überprüfung von gesendeten E-Mail-Nachrichten auf wurmähnliche Aktivitäten:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Erweitert** und anschließend auf die Registerkarte **E-Mail**.
3. Klicken Sie auf **WormStopper aktivieren (empfohlen)** (Abbildung 2-3).

   Standardmäßig sind folgende Detailoptionen aktiviert:

   - Mustervergleich zur Erkennung verdächtiger Aktivität
   - Warnung beim Senden einer E-Mail an 40 oder mehr Empfänger
   - Warnung beim Senden von 5 oder mehr E-Mails innerhalb von 30 Sekunden

   HINWEIS
   Wenn Sie die Anzahl der Empfänger oder die Dauer für die Überprüfung gesendeter E-Mails ändern, kann es zu ungültigen (fehlerhaften) Erkennungen kommen. McAfee empfiehlt, die Standardeinstellung durch Klicken auf **Nein** beizubehalten. Andernfalls können Sie auf **Ja** klicken und die Standardeinstellung durch Ihre bevorzugte Einstellung ersetzen.

Diese Option kann automatisch aktiviert werden, nachdem zum ersten Mal ein potentieller Wurm entdeckt wurde (ausführliche Informationen finden Sie unter *Verwalten potentieller Würmer* auf Seite 32):

- Automatische Blockierung verdächtiger, ausgehender E-Mails

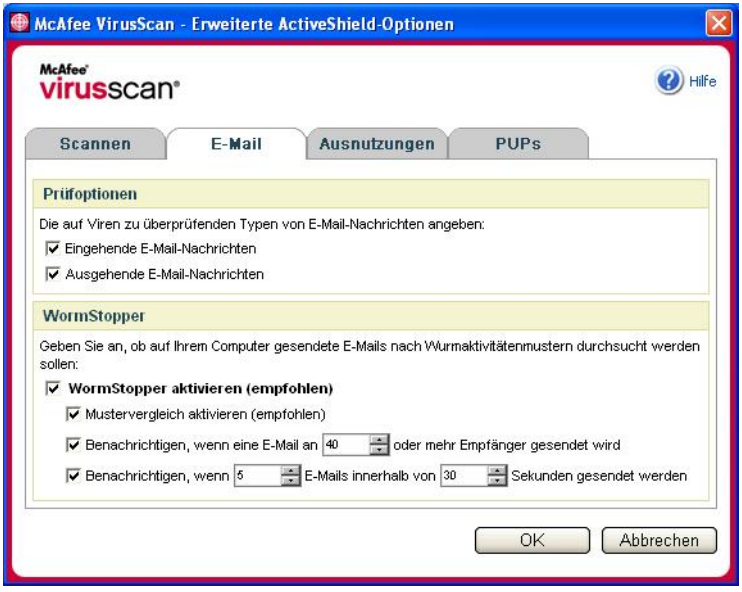


Abbildung 2-3. Erweiterte ActiveShield-Optionen - Registerkarte „E-Mail“

Prüfen von Anlagen eingehender Instant Messages

Standardmäßig wird die Überprüfung von Instant Messages-Anlagen über die Option **Anlagen von eingehenden Instant Messages überprüfen** (Abbildung 2-1 auf Seite 20) aktiviert.

Wenn diese Option aktiviert ist, führt VirusScan automatisch die Virenprüfung durch und versucht, eingehende infizierte Instant Messages-Anlagen für den Großteil gängiger Instant Messaging-Programme zu bereinigen. Hierzu zählen:

- MSN Messenger 6.0 oder höher
- Yahoo Messenger 4.1 oder höher
- AOL Instant Messenger 2.1 oder höher

HINWEIS

Aus Sicherheitsgründen kann die automatische Bereinigung von Instant Messages-Anlagen nicht deaktiviert werden.

Wenn eine eingehende Instant Messages-Anlage infiziert ist, führt VirusScan folgende Schritte durch:

- Es wird versucht, die infizierte Nachricht zu bereinigen
- Sie werden aufgefordert, die Nachricht, die nicht bereinigt werden kann, unter Quarantäne zu stellen oder zu löschen

Prüfen aller Dateien

Wenn Sie in ActiveShield die Standardeinstellung **Alle Dateien (empfohlen)** verwenden, werden alle Dateitypen durchsucht, auf die der Computer zugreift. Verwenden Sie diese Option, um die genaueste Prüfung durchzuführen.

So konfigurieren Sie ActiveShield für die Überprüfung aller Dateitypen:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Erweitert**, und aktivieren Sie dann die Registerkarte **Scannen** (Abbildung 2-4 auf Seite 26).
3. Klicken Sie auf **Alle Dateien (empfohlen)** und dann auf **OK**.

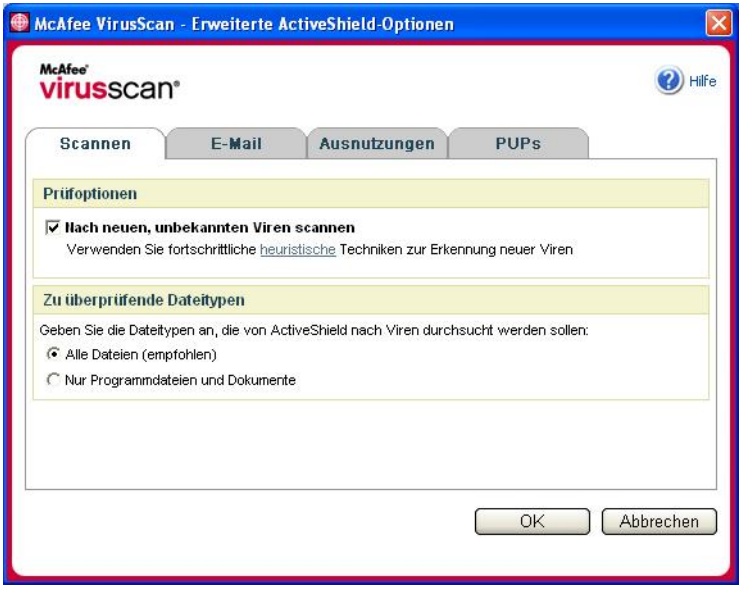


Abbildung 2-4. Erweiterte ActiveShield-Optionen – Registerkarte „Scannen“

Ausschließliches Prüfen von Programmdateien und Dokumenten

Wenn Sie in ActiveShield die Option **Nur Programmdateien und Dokumente** auswählen, werden Programmdateien und Dokumente durchsucht, nicht jedoch andere auf Ihrem Computer verwendete Dateien. Durch die jeweils neueste Virussignaturdatei (DAT-Datei) wird bestimmt, welche Dateitypen von ActiveShield durchsucht werden. So lassen Sie in ActiveShield nur Programmdateien und Dokumente überprüfen:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Erweitert**, und aktivieren Sie dann die Registerkarte **Scannen** (Abbildung 2-4).
3. Klicken Sie auf **Nur Programmdateien und Dokumente** und dann auf **OK**.

Prüfen auf neue, unbekannte Viren

Wenn Sie ActiveShield so konfigurieren, dass die Standardoption **Nach neuen, unbekannten Viren scannen (empfohlen)** verwendet wird, werden erweiterte heuristische Techniken verwendet, anhand derer eine Übereinstimmung zwischen den Dateien und Signaturen bekannter Viren ermittelt werden soll. Gleichzeitig wird versucht, nicht identifizierte Viren in den Dateien anhand bestimmter Anzeichen zu ermitteln..

So konfigurieren Sie ActiveShield für die Prüfung auf neue, unbekannte Viren:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Erweitert**, und aktivieren Sie dann die Registerkarte **Scannen** (Abbildung 2-4).
3. Klicken Sie auf **Nach neuen, unbekannten Viren scannen (empfohlen)** und dann auf **OK**.

Prüfen auf Skripts

VirusScan überwacht den Computer auf verdächtige Aktivitäten, die möglicherweise darauf hinweisen, dass Ihr Computer akut gefährdet ist. Durch VirusScan werden Viren bereinigt, durch ScriptStopper™ hingegen wird verhindert, dass trojanische Pferde Skripts ausführen, mit denen Viren weiterverbreitet werden.

Ein trojanisches Pferd ist ein bösartiges Programm, das als nützliche Anwendung getarnt ist. Trojanische Pferde sind keine Viren, da sie sich nicht fortpflanzen, können aber eine ähnlich destruktive Wirkung entfalten wie Viren.

Durch den ScriptStopper-Schutzmechanismus werden bösartige Aktivitäten erkannt, gemeldet und blockiert. Zu verdächtigen Aktivitäten auf dem Computer zählt Folgendes:

- Eine Skriptausführung, die dazu führt, dass Dateien erstellt, kopiert oder gelöscht werden bzw. dass die Windows-Registrierung geöffnet wird.

Wenn Sie ActiveShield so einstellen, dass die Standardoption **ScriptStopper aktivieren (empfohlen)** im Dialogfeld **Erweiterte Optionen** verwendet wird, überwacht ScriptStopper die Skriptausführung auf verdächtige Muster und gibt eine Warnung aus, wenn eine festgelegte Anzahl an E-Mails oder Empfängern innerhalb eines festgelegten Intervalls überschritten wird.

So konfigurieren Sie ActiveShield für die Prüfung von ausgeführten Skripts auf wurmähnliche Aktivitäten:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Erweitert**, und aktivieren Sie dann die Registerkarte **Ausnutzungen** (Abbildung 2-5).
3. Klicken Sie auf **ScriptStopper aktivieren (empfohlen)** und dann auf **OK**.

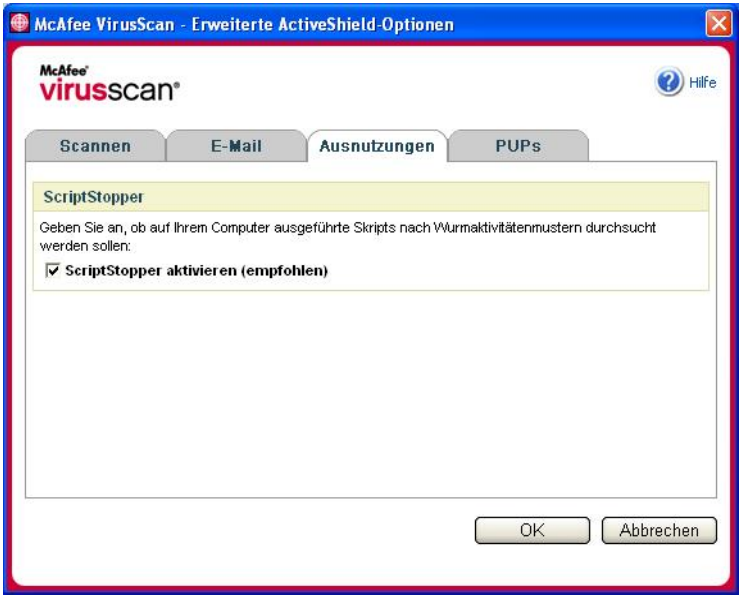


Abbildung 2-5. Erweiterte ActiveShield-Optionen – Registerkarte „Ausnutzungen“

Prüfen auf möglicherweise unerwünschte Programme (PUPs)

HINWEIS
Wenn McAfee AntiSpyware auf Ihrem Computer installiert ist, verwaltet es alle Aktivitäten von möglicherweise unerwünschten Programmen. Öffnen Sie McAfee AntiSpyware zur Konfiguration der Optionen.

Wenn Sie ActiveShield so konfigurieren, dass die standardmäßige Option **Auf möglicherweise unerwünschte Programme überprüfen (empfohlen)** im Dialogfeld **Erweiterte Optionen** aktiviert ist, entdeckt, blockiert und entfernt der Schutz vor möglicherweise unerwünschten Programmen (PUP) rasch Spyware, Adware und andere böswillige Programme, die Ihre persönlichen Daten sammeln und ohne Ihre Zustimmung weiterleiten.

So konfigurieren Sie ActiveShield für die Überprüfung auf PUPs:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Erweitert**, und aktivieren Sie dann die Registerkarte **PUPs** (Abbildung 2-6).
3. Klicken Sie auf **Auf möglicherweise unerwünschte Programme überprüfen (empfohlen)** und dann auf **OK**.

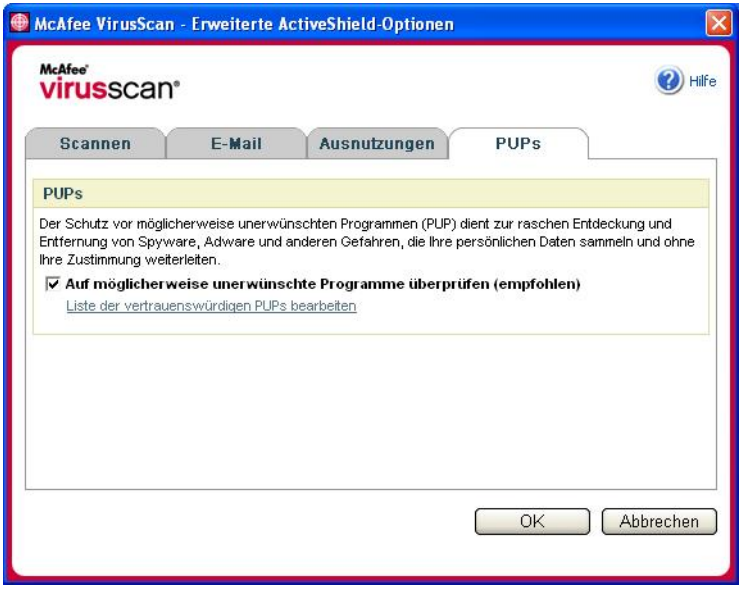


Abbildung 2-6. Erweiterte ActiveShield-Optionen – Registerkarte „PUPs“

Übersicht über Sicherheitswarnungen

Wenn ActiveShield einen Virus findet, wird eine Viruswarnung ausgegeben, die Abbildung 2-7 ähnelt. Bei den meisten Viren, Trojanern und Würmern versucht ActiveShield automatisch, die Datei zu bereinigen, und zeigt eine Warnung an. Bei möglicherweise unerwünschten Programmen (PUPs) entdeckt ActiveShield die Datei, blockiert sie automatisch und zeigt eine Warnung an.

McAfee VirusScan
Virus gefunden
Die Datei C:\Dokumente und Einstellungen\Administrator\Lokale Einstell... ist mit dem Virus EICAR test file infiziert und kann nicht gereinigt werden.
Ich möchte...
Infizierte Datei löschen
Infizierte Datei unter Quarantäne stellen
Weitere Informationen
Aktuelle Tätigkeit fortsetzen

Abbildung 2-7. Viruswarnung

Anschließend können Sie angeben, wie mit infizierten Dateien, infizierten E-Mails, verdächtigen Skripts, potentiellen Würmern oder PUPs verfahren werden soll, und ob infizierte Dateien zu Forschungszwecken an die McAfee AVERT-Laboratorien übermittelt werden sollen.

Wenn ActiveShield eine verdächtige Datei entdeckt, werden Sie aufgefordert, den Computer sofort vollständig zu überprüfen, um zusätzlichen Schutz zu gewährleisten. Wenn Sie die Aufforderung zum Überprüfen Ihres Computers nicht ausblenden, werden Sie solange in regelmäßigen Abständen daran erinnert, bis Sie die Überprüfung durchführen.

Verwalten infizierter Dateien

1 Wenn ActiveShield die Datei bereinigen kann, können Sie sich ausführlicher informieren oder die Warnung ignorieren:

- Klicken Sie auf **Weitere Informationen**, um den Dateinamen, den Speicherort und den Virusnamen für die infizierte Datei anzuzeigen.
- Klicken Sie auf **Fortfahren**, um die Warnung zu ignorieren und zu schließen.

2 Wenn ActiveShield die Datei nicht bereinigen kann, klicken Sie auf **Infizierte Datei unter Quarantäne stellen**, um infizierte und verdächtige Dateien zu verschlüsseln und im Quarantäneverzeichnis vorübergehend unter Quarantäne zu stellen, bis eine angemessene Maßnahme ergriffen werden kann.

   Es wird eine Bestätigungsmeldung angezeigt, die Sie zum Überprüfen Ihres Computers auf Viren auffordert. Klicken Sie auf **Scan**, um den Quarantäneprozess abzuschließen.

3 Wenn ActiveShield die Datei nicht unter Quarantäne stellen kann, klicken Sie auf **Infizierte Datei löschen**, um zu versuchen, die Datei zu entfernen.

Verwalten infizierter E-Mails

Standardmäßig wird bei der E-Mail-Überprüfung automatisch versucht, infizierte E-Mail-Nachrichten zu bereinigen. Es wird eine Warnungsdatei in die eingehende E-Mail aufgenommen, die Sie darüber informiert, ob die E-Mail-Nachricht bereinigt, unter Quarantäne gestellt oder gelöscht wurde.

Verwalten verdächtiger Skripts

Wenn ActiveShield ein verdächtiges Skript erkennt, können Sie sich ausführlicher informieren und das Skript dann anhalten, wenn Sie nicht beabsichtigt hatten, es auszuführen:

- Klicken Sie auf **Weitere Informationen**, um den Namen, den Speicherort und die Beschreibung der Aktivität anzuzeigen, die mit dem verdächtigen Skript in Verbindung steht.
- Mit **Dieses Skript anhalten** können Sie die Ausführung des verdächtigen Skripts unterbinden.

Wenn Sie das Skript als vertrauenswürdig einschätzen, können Sie seine Ausführung zulassen:

- Klicken Sie auf **Dieses Mal alle Skripts zulassen** , um alle in einer einzelnen Datei enthaltenen Skripts dieses eine Mal auszuführen.
- Klicken Sie auf **Fortfahren**, um die Warnung zu ignorieren und das Skript ausführen zu lassen.

Verwalten potentieller Würmer

Wenn ActiveShield einen potentiellen Wurm erkennt, können Sie sich ausführlicher informieren und die E-Mail-Aktivität dann anhalten, wenn Sie nicht beabsichtigt hatten, sie zu initiieren:

- Klicken Sie auf **Weitere Informationen**, um die Empfängerliste, die Betreffzeile, den Nachrichtentext und die Beschreibung der verdächtigen Aktivität anzuzeigen, die mit der infizierten E-Mail-Nachricht in Verbindung steht.
- Mit **E-Mail anhalten** können Sie verhindern, dass die verdächtige E-Mail gesendet wird. Löschen Sie sie aus der Nachrichtenwarteschlange.

Wenn Sie die E-Mail-Aktivität als vertrauenswürdig einschätzen, klicken Sie auf **Fortfahren**, um die Warnung zu ignorieren und das Senden der E-Mail zuzulassen.

Verwalten von PUPs

Wenn ActiveShield ein möglicherweise unerwünschtes Programm (PUP) erkennt und blockiert, können Sie sich ausführlicher informieren und das Programm dann entfernen, wenn Sie nicht beabsichtigt hatten, es zu installieren:

- Klicken Sie auf **Weitere Informationen**, um den Namen, den Speicherort und die empfohlene Vorgehensweise für dieses PUP anzuzeigen.
- Klicken Sie auf **PUP entfernen**, um das Programm zu entfernen, wenn Sie nicht beabsichtigt hatten, es zu installieren.

  Es wird eine Bestätigungsmeldung angezeigt.

  - Wenn Sie (a) das PUP nicht erkennen oder (b) das PUP nicht als Teil einer Programmgruppe installiert oder den Lizenzvertrag in Verbindung mit solchen Programmen nicht akzeptiert haben, klicken Sie auf **OK**, um das Programm mithilfe der Entfernungsmethode von McAfee zu entfernen.

  - Klicken Sie andernfalls auf **Abbrechen**, um den automatischen Entfernungsvorgang zu beenden. Wenn Sie Ihre Meinung später ändern, können Sie das Programm mithilfe des Deinstallationsprogramms des Herstellers manuell entfernen.
- Klicken Sie auf **Fortfahren**, um die Warnung zu ignorieren und das Programm dieses Mal zu blockieren.

Wenn Sie (a) das PUP erkennen oder (b) das PUP als Teil einer Programmgruppe installiert oder den Lizenzvertrag in Verbindung mit solchen Programmen akzeptiert haben, können Sie es ausführen.

- Klicken Sie auf **Dieses PUP als vertrauenswürdig einstufen**, um das Programm in die Liste der vertrauenswürdigen Programme aufzunehmen und seine Ausführung immer zuzulassen.

  Nähere Informationen dazu finden Sie unter *Verwalten von vertrauenswürdigen PUPs*.

Verwalten von vertrauenswürdigen PUPs

Die Programme, die Sie zur Liste der vertrauenswürdigen PUPs hinzufügen, werden von McAfee VirusScan nicht entdeckt.

Wenn ein PUP entdeckt und zur Liste der vertrauenswürdigen PUPs hinzugefügt wird, können Sie es später bei Bedarf wieder aus der Liste entfernen.

Wenn die Liste der vertrauenswürdigen PUPs voll ist, müssen Sie einige Objekte aus der Liste entfernen, bevor Sie einem weiteren PUP vertrauen können.

So entfernen Sie ein Programm aus der Liste der vertrauenswürdigen PUPs:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Erweitert**, und aktivieren Sie dann die Registerkarte **PUPs**.
3. Klicken Sie auf **Liste der vertrauenswürdigen PUPs bearbeiten**, aktivieren Sie das Kontrollkästchen vor dem Dateinamen, und klicken Sie auf **Entfernen**. Klicken Sie auf **OK**, wenn Sie die gewünschten Objekte entfernt haben.

Manuelles Überprüfen des Computers

Mit der Scan-Funktion werden Festplatten, Disketten sowie einzelne Dateien und Ordner nach Viren und möglicherweise unerwünschten Programmen durchsucht. Wenn bei der Überprüfung eine infizierte Datei gefunden wird, wird automatisch versucht, die Datei zu bereinigen, sofern es sich dabei nicht um ein möglicherweise unerwünschtes Programm handelt. Wenn Scan die Datei nicht bereinigen kann, können Sie die Datei unter Quarantäne stellen oder löschen.

Manuelles Überprüfen auf Viren und andere Bedrohungen

So überprüfen Sie Ihren Computer:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Auf Viren überprüfen**.

   Das Dialogfeld **Auf Viren überprüfen** wird angezeigt (Abbildung 2-8).

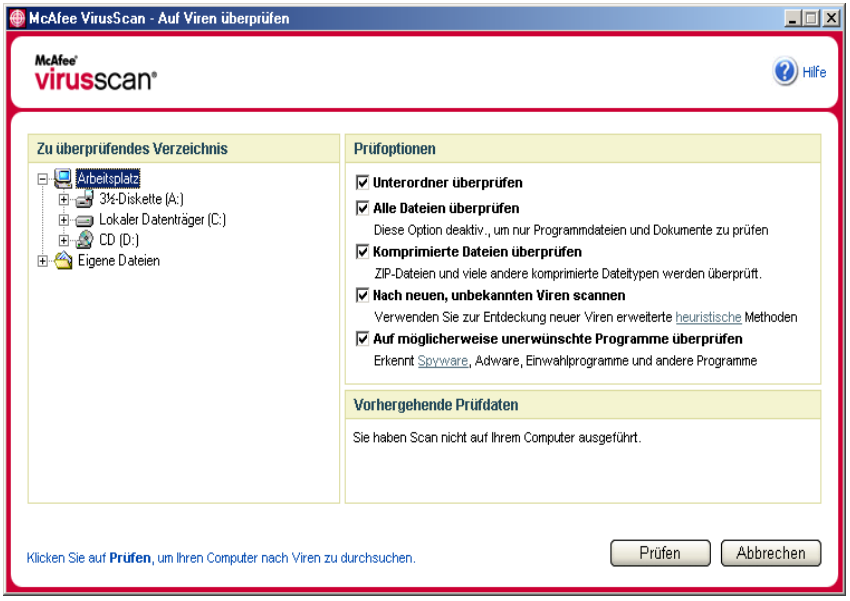


Abbildung 2-8. Dialogfeld „Auf Viren überprüfen“

2 Klicken Sie auf das Laufwerk, den Ordner oder die Datei, die überprüft werden soll.

3 Wählen Sie die **Prüfoptionen** aus. Standardmäßig sind für eine möglichst gründliche Überprüfung alle verfügbaren **Prüfoptionen** aktiviert (Abbildung 2-8):

- **Unterordner überprüfen**: Verwenden Sie diese Option, um Dateien in Unterordnern auf Viren zu durchsuchen. Deaktivieren Sie dieses Kontrollkästchen, wenn nur die Dateien durchsucht werden sollen, die beim Öffnen eines Ordners oder Laufwerks angezeigt werden.

  Beispiel: Wenn Sie das Kontrollkästchen **Unterordner überprüfen** deaktivieren, werden ausschließlich die Dateien in Abbildung 2-9 durchsucht. Die Ordner und ihr Inhalt werden nicht überprüft. Wenn sie ebenfalls durchsucht werden sollen, belassen Sie das Kontrollkästchen aktiviert.

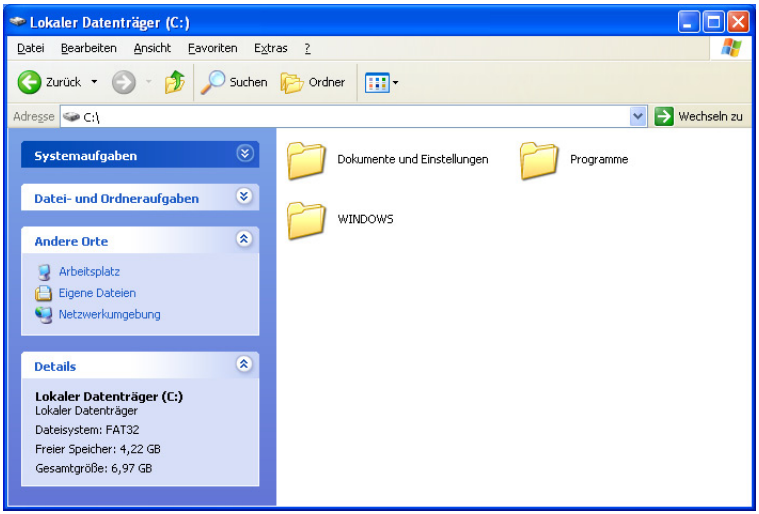


Abbildung 2-9. Inhalt lokaler Datenträger

- **Alle Dateien überprüfen**: Verwenden Sie diese Option, um eine umfassende Überprüfung aller Dateitypen zu gewährleisten. Deaktivieren Sie dieses Kontrollkästchen, um den Vorgang zu beschleunigen und nur Programmdateien und Dokumente zu durchsuchen.

- **Komprimierte Dateien überprüfen**: Verwenden Sie diese Option, um verborgene infizierte Dateien in ZIP-Dateien und anderen komprimierten Dateien einzublenden. Deaktivieren Sie dieses Kontrollkästchen, um die Überprüfung jeglicher Dateien oder komprimierter Dateien in der komprimierten Datei zu unterbinden.

  Manchmal werden Viren in eine ZIP-Datei eingesetzt und diese ZIP-Datei wiederum in eine weitere ZIP-Datei eingefügt, um Anti-Virus-Scanner zu umgehen. Wenn Sie diese Option aktiviert belassen, kann Scan diese Viren ermitteln.

- **Nach neuen, unbekannten Viren scannen** : Verwenden Sie diese Option, um die neuesten Viren zu ermitteln, für die es möglicherweise noch kein Gegenmittel gibt. Diese Option verwendet erweiterte heuristische Techniken, anhand derer eine Übereinstimmung zwischen den Dateien und Signaturen bekannter Viren ermittelt werden soll. Gleichzeitig wird versucht, anhand bestimmter Anzeichen nicht identifizierte Viren in den Dateien zu ermitteln.

Bei diesem Scan-Verfahren wird auch nach charakteristischen Merkmalen in Dateien gesucht, die eine Virusinfektion prinzipiell ausschließen. Dadurch wird weitgehend verhindert, dass Scan falsche Meldungen ausgibt. Wenn mit dem heuristischen Verfahren jedoch ein Virus in einer Datei gefunden wird, sollten Sie dieselben Maßnahmen ergreifen wie bei einem bekannten Virus.

Diese Option bietet eine äußerst gründliche Prüfung, die jedoch zeitaufwendiger als eine normale Prüfung ist.

- **Auf möglicherweise unerwünschte Programme überprüfen** : Verwenden Sie diese Option, um Spyware, Adware, Dialer und andere Programme ausfindig zu machen, die nicht auf Ihrem Computer installiert werden sollten.

  HINWEIS
  Lassen Sie alle Optionen aktiviert, um die Überprüfung so gründlich wie möglich zu gestalten. Dadurch dauert die Überprüfung etwas länger, aber jede Datei im gewählten Laufwerk oder Ordner wird effektiv überprüft. Je größer die Festplatte ist und je mehr Dateien Sie haben, desto länger dauert die Überprüfung.

4 Klicken Sie auf **Scan** , um mit dem Überprüfen der Dateien zu beginnen.

Nach Abschluss der Überprüfung wird in einer Zusammenfassung angezeigt, wie viele Dateien überprüft und erkannt wurden, wie viele möglicherweise unerwünschte Programme gefunden wurden und wie viele erkannte Dateien automatisch bereinigt wurden.

5 Klicken Sie auf **OK**, um die Zusammenfassung zu schließen und die Liste der erkannten Dateien im Dialogfeld **Auf Viren überprüfen** anzuzeigen (Abbildung 2-10).

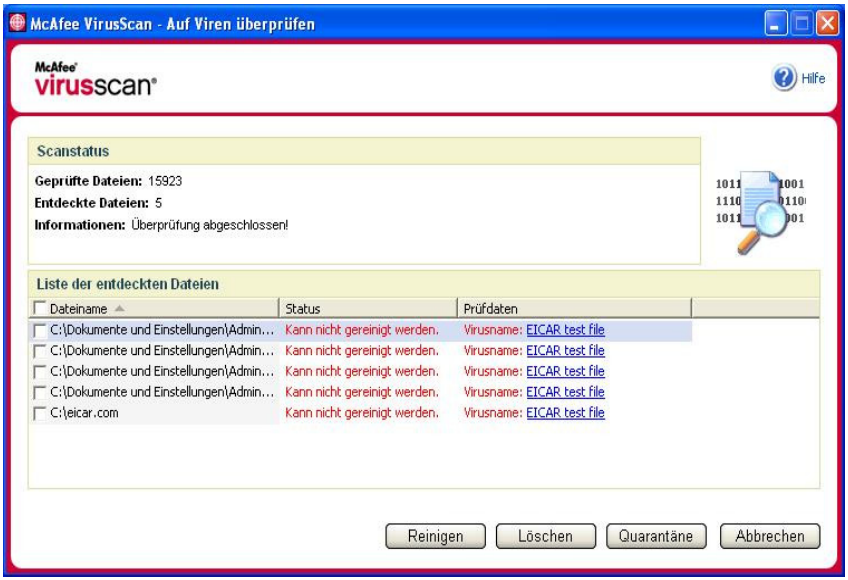


Abbildung 2-10. Prüfergebnisse

HINWEIS
Unter **Geprüfte Dateien** zählt Scan komprimierte Dateien (ZIP, CAB usw.) jeweils als eine Datei. Die Anzahl der durchsuchten Dateien kann variieren, wenn Sie Ihre temporären Internetdateien seit Ihrer letzten Überprüfung gelöscht haben.

6 Wenn Scan keine Viren oder möglicherweise unerwünschten Programme ermittelt, klicken Sie auf **Zurück**, um ein anderes Laufwerk oder einen anderen Ordner zur Überprüfung auszuwählen, oder auf **Schließen**, um das Dialogfeld zu schließen. Informieren Sie sich andernfalls unter *Übersicht über Bedrohungserkennungen* auf Seite 40.

Prüfen über Windows-Explorer

VirusScan ermöglicht die Verwendung eines Kontextmenüs, mit dem ausgewählte Dateien, Ordner oder Laufwerke über Windows-Explorer auf Viren und möglicherweise unerwünschte Programme geprüft werden können.

So überprüfen Sie Dateien in Windows-Explorer:

1 Öffnen Sie Windows-Explorer.

2 Klicken Sie mit der rechten Maustaste auf das Laufwerk, den Ordner oder die Datei, die überprüft werden soll, und klicken Sie dann auf **Auf Viren überprüfen**.

Das Dialogfeld **Auf Viren überprüfen** wird angezeigt, und es wird mit der Überprüfung der Dateien begonnen. Standardmäßig sind für eine möglichst gründliche Überprüfung alle verfügbaren **Prüfoptionen** aktiviert (Abbildung 2-8 auf Seite 34).

Prüfen über Microsoft Outlook

VirusScan stellt ein Symbol auf der Symbolleiste bereit, mit dem ausgewählte Nachrichtenspeicher und die zugehörigen Unterordner, Mailbox-Ordner bzw. E-Mail-Nachrichten mit Anlagen in Microsoft Outlook 97 (oder höher) auf Viren und möglicherweise unerwünschte Programme überprüft werden können.

So überprüfen Sie E-Mails in Microsoft Outlook:

1 Öffnen Sie Microsoft Outlook.

2 Klicken Sie auf den Nachrichtenspeicher, Ordner oder die E-Mail-Nachricht mit Anlage, die überprüft werden soll, und klicken Sie dann auf der Symbolleiste auf das E-Mail-Scan-Symbol .

Der E-Mail-Scanner wird geöffnet und beginnt mit der Überprüfung von Dateien. Standardmäßig sind für eine möglichst gründliche Überprüfung alle verfügbaren **Prüfoptionen** aktiviert (Abbildung 2-8 auf Seite 34).

Automatisches Überprüfen auf Viren und andere Bedrohungen

Obwohl VirusScan Dateien überprüft, wenn Sie oder Ihr Computer darauf zugreifen, können Sie im Windows-Taskplaner die automatische Überprüfung planen, um den Computer in festgelegten Intervallen gründlich nach Viren und möglicherweise unerwünschten Programmen zu durchsuchen.

So planen Sie eine Prüfung:

1 Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Optionen**.

Das Dialogfeld **VirusScan-Optionen** wird geöffnet.

2 Klicken Sie auf die Registerkarte **Geplante Prüfung** (Abbildung 2-11 auf Seite 39).

Abbildung 2-11. Optionen für geplante Prüfungen

3 Aktivieren Sie das Kontrollkästchen **Computer zu einem festgelegten Zeitpunkt überprüfen** , um die automatische Prüfung zu aktivieren.

4 Legen Sie einen Zeitplan für die automatische Prüfung fest:

- Wenn Sie den standardmäßigen Zeitplan (freitags um 20 Uhr) akzeptieren möchten, klicken Sie auf **OK**.
- So bearbeiten Sie den Zeitplan:

  a. Klicken Sie auf **Bearbeiten**.

  b. Wählen Sie in der Liste **Task planen**, wie oft Ihr Computer überprüft werden soll, und wählen Sie dann weitere Optionen in dem darunter liegenden dynamischen Bereich aus:

  Täglich: Geben Sie die Anzahl der Tage zwischen Scans an.

  Wöchentlich (Standardeinstellung): Geben Sie die Anzahl der Wochen zwischen den Scans und die Wochentage an, an denen die Scans ausgeführt werden sollen.

  Monatlich: Geben Sie den Tag an, an dem der Scan ausgeführt werden soll. Klicken Sie auf **Monate auswählen**, um die Monate auszuwählen, in denen gescannt werden soll, und klicken Sie dann auf **OK**.

Einmalig: Geben Sie das Datum an, an dem der Scan ausgeführt werden soll.

HINWEIS
Folgende Optionen im Windows-Taskplaner werden nicht unterstützt:
Beim Systemstart, **Im Leerlauf** und **Mehrfache Zeitpläne anzeigen**. Der letzte unterstützte Zeitplan bleibt so lange aktiv, bis Sie eine gültige Option auswählen.

c. Wählen Sie im Feld **Beginn um** die Tageszeit aus, zu der die Überprüfung des Computers erfolgen soll.

d. Wenn Sie erweiterte Optionen einstellen möchten, klicken Sie auf **Erweitert**.

Das Dialogfeld **Erweiterte Planungsoptionen** wird angezeigt.

i. Geben Sie Anfangsdatum, Enddatum, Dauer und Endzeitpunkt ein, und geben Sie an, ob der Scan-Vorgang zur festgelegten Zeit beendet werden soll, wenn die Überprüfung noch nicht beendet ist.

ii. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und das Dialogfeld zu schließen. Klicken Sie andernfalls auf **Abbrechen**.

5 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und das Dialogfeld zu schließen. Klicken Sie andernfalls auf **Abbrechen**.

6 Wenn Sie zum standardmäßigen Zeitplan zurückkehren möchten, klicken Sie auf **Auf Standard setzen**. Klicken Sie andernfalls auf **OK**.

Übersicht über Bedrohungserkennungen

Bei den meisten Viren, Trojanern und Würmern versucht Scan automatisch, die Datei zu bereinigen. Anschließend können Sie angeben, wie mit erkannten Dateien verfahren werden soll, und ob sie zu Forschungszwecken an die McAfee AVERT-Labore übermittelt werden sollen. Wenn die Scan-Funktion ein möglicherweise unerwünschtes Programm findet, können Sie versuchen, es manuell zu bereinigen, unter Quarantäne zu stellen oder zu löschen (Einsenden an AVERT ist nicht möglich).

So gehen Sie mit einem Virus oder möglicherweise unerwünschten Programm vor:

1 Wenn eine Datei in der **Liste der erkannten Dateien** angezeigt wird, aktivieren Sie das Kontrollkästchen vor der Datei.

HINWEIS
Wenn in der Liste mehrere Dateien angezeigt werden, können Sie das Kontrollkästchen vor der Liste **Dateiname** aktivieren, um denselben Vorgang für sämtliche Dateien durchzuführen. Sie können auch auf den Dateinamen in der Liste **Prüfdaten** klicken, um Details aus der Virus Information Library anzuzeigen.

2 Wenn es sich bei der Datei um ein möglicherweise unerwünschtes Programm handelt, können Sie auf **Reinigen** klicken, um sie zu bereinigen.

3 Wenn Scan die Datei nicht bereinigen kann, klicken Sie auf **Quarantäne**, um infizierte und verdächtige Dateien zu verschlüsseln und im Quarantäneverzeichnis vorübergehend unter Quarantäne zu stellen, bis eine angemessene Maßnahme ergriffen werden kann. (Nähere Informationen dazu finden Sie unter *Verwalten von Dateien unter Quarantäne* auf Seite 41.)

4 Wenn Scan die Datei nicht bereinigen oder unter Quarantäne stellen kann, haben Sie folgende Möglichkeiten:

- Klicken Sie auf **Löschen**, um die Datei zu entfernen.
- Klicken Sie auf **Abbrechen**, um das Dialogfeld zu schließen, ohne weitere Maßnahmen zu ergreifen.

Wenn Scan die erkannte Datei weder bereinigen noch löschen kann, rufen Sie die Virus Information Library unter http://us.mcafee.com/virusInfo/default.asp auf. Dort finden Sie Anweisungen zum manuellen Löschen der Datei.

Wenn die erkannte Datei das Herstellen einer Internetverbindung verhindert bzw. Sie Ihren Computer nicht mehr verwenden können, starten Sie den Computer mit einer Rettungsdiskette. In vielen Fällen kann ein infizierter Computer über die Rettungsdiskette wieder gestartet werden. Nähere Informationen dazu finden Sie unter *Erstellen einer Rettungsdiskette* auf Seite 43.

Weitere Hilfe erhalten Sie vom McAfee-Kundendienst unter http://www.mcafeehelp.com/

Verwalten von Dateien unter Quarantäne

Mithilfe der Quarantäne-Funktion können Sie infizierte und verdächtige Dateien verschlüsseln und temporär in einem Quarantäneverzeichnis unter Quarantäne stellen, bis eine angemessene Maßnahme ergriffen werden kann. Nach der Bereinigung können unter Quarantäne gestellte Dateien am ursprünglichen Speicherort wiederhergestellt werden.

So verwalten Sie eine unter Quarantäne gestellte Datei:

1 Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Dateien unter Quarantäne verwalten**.

Eine Liste mit Dateien unter Quarantäne wird angezeigt (Abbildung 2-12).

Abbildung 2-12. Dialogfeld „Dateien unter Quarantäne verwalten“

2 Aktivieren Sie das Kontrollkästchen neben den Dateien, die bereinigt werden sollen.

> **HINWEIS**
> Wenn in der Liste mehrere Dateien angezeigt werden, können Sie das Kontrollkästchen vor der Liste **Dateiname** aktivieren, um denselben Vorgang für sämtliche Dateien durchzuführen. Sie können auch auf den Virusnamen in der Liste **Status** klicken, um Details aus der Virus Information Library anzuzeigen.
>
> Alternativ klicken Sie auf **Hinzufügen**, wählen Sie eine verdächtige Datei aus, die der Quarantäneliste hinzugefügt werden soll, klicken Sie auf **Öffnen** und wählen die Datei dann in der Quarantäneliste aus.

3 Klicken Sie auf **Reinigen**.

4 Wenn die Datei bereinigt ist, klicken Sie auf **Wiederherstellen**, um die Datei wieder an ihren ursprünglichen Speicherort zu verschieben.

5 Wenn VirusScan den Virus nicht bereinigen kann, klicken Sie auf **Löschen**, um die Datei zu entfernen.

6 Wenn VirusScan die Datei nicht bereinigen oder löschen kann und es sich nicht um ein möglicherweise unerwünschtes Programm handelt, können Sie die Datei zu Forschungszwecken an das McAfee AntiVirus Emergency Response Team (AVERT™) übermitteln:

   a Aktualisieren Sie die Virussignaturdateien, wenn sie älter als zwei Wochen sind.

   b Überprüfen Sie Ihr Abonnement.

   c Wählen Sie die Datei aus, und klicken Sie auf **Senden**, um die Datei an AVERT zu übermitteln.

   VirusScan sendet die unter Quarantäne gestellte Datei als Anlage einer E-Mail-Nachricht, die Ihre E-Mail-Adresse, Ihr Land, die Softwareversion, das Betriebssystem sowie den ursprünglichen Namen und Speicherort der Datei enthält. Pro Tag darf maximal eine Datei mit 1,5 MB übermittelt werden.

7 Klicken Sie auf **Abbrechen**, um das Dialogfeld zu schließen, ohne weitere Maßnahmen zu ergreifen.

Erstellen einer Rettungsdiskette

Bei Rescue Disk handelt es sich um ein Dienstprogramm, das eine startfähige Diskette erstellt, über die Sie einen infizierten Computer starten und nach Viren durchsuchen können.

> **HINWEIS**
> Um die Imagedatei für die Rettungsdiskette herunterladen zu können, müssen Sie mit dem Internet verbunden sein. Rescue Disk ist nur für Computer mit FAT-Partitionen (FAT 16 und FAT 32) verfügbar und ist für NTFS-Partitionen nicht erforderlich.

So erstellen Sie eine Rettungsdiskette:

1 Legen Sie eine nicht infizierte Diskette in Laufwerk A eines nicht infizierten Computers ein. Verwenden Sie Scan, wenn Sie sicherstellen möchten, dass der Computer und die Diskette nicht von einem Virus befallen sind. (Nähere Informationen dazu finden Sie unter *Manuelles Überprüfen auf Viren und andere Bedrohungen* auf Seite 33.)

2 Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Rettungsdiskette erstellen**.

Das Dialogfeld **Rettungsdiskette erstellen** wird angezeigt (Abbildung 2-13).

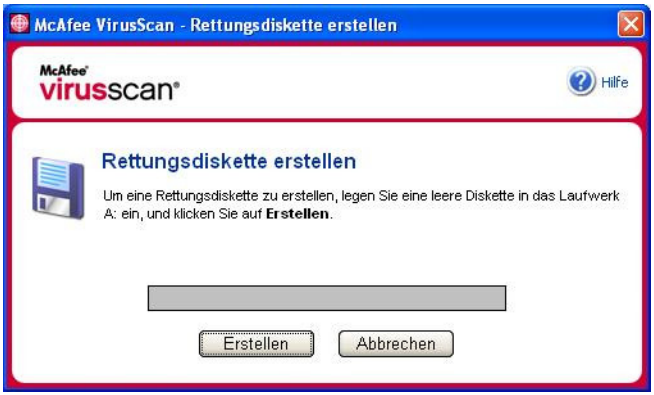

McAfee VirusScan - Rettungsdiskette erstellen
McAfee
virusscan
Hilfe
Rettungsdiskette erstellen
Um eine Rettungsdiskette zu erstellen, legen Sie eine leere Diskette in das Laufwerk A: ein, und klicken Sie auf Erstellen.
Erstellen
Abbrechen

Abbildung 2-13. Dialogfeld „Rettungsdiskette erstellen“

3 Klicken Sie auf **Erstellen**, um die Rettungsdiskette zu erstellen.

Wenn Sie zum ersten Mal eine Rettungsdiskette erstellen, werden Sie in einer Meldung darüber informiert, dass die Imagedatei für die Rettungsdiskette heruntergeladen werden muss. Klicken Sie auf **OK**, um die Komponente jetzt herunterzuladen, oder auf **Abbrechen** für einen späteren Download.

Es wird eine Warnung angezeigt, die Sie darüber informiert, dass der Inhalt der Diskette verloren geht.

4 Klicken Sie auf **Ja**, um die Rettungsdiskette zu erstellen.

Der Status für diesen Vorgang wird im Dialogfeld **Rettungsdiskette erstellen** angegeben.

5 Wenn die erfolgreiche Erstellung einer Rettungsdiskette gemeldet wird, klicken Sie auf **OK**, und schließen Sie dann das Dialogfeld **Rettungsdiskette erstellen**.

6 Nehmen Sie die Rettungsdiskette aus dem Laufwerk, versehen Sie sie mit einem Schreibschutz, und bewahren Sie den Datenträger an einem sicheren Ort auf.

Einrichten des Schreibschutzes für eine Rettungsdiskette

So richten Sie den Schreibschutz für eine Rettungsdiskette ein:

1 Drehen Sie die Diskette mit der Beschriftungsseite nach unten (die runde Metallplatte ist sichtbar).

2 Suchen Sie den Riegel für den Schreibschutz. Verschieben Sie den Riegel so, dass die Öffnung sichtbar ist.

Verwenden einer Rettungsdiskette

So verwenden Sie eine Rettungsdiskette:

1. Schalten Sie den infizierten Computer aus.
2. Legen Sie die Rettungsdiskette in das Laufwerk ein.
3. Schalten Sie den Computer wieder ein.

   Es wird ein graues Fenster mit verschiedenen Optionen geöffnet.
4. Wählen Sie die Option, die Ihren Bedürfnissen am ehesten entspricht, indem Sie die Funktionstasten (F2, F3 usw.) drücken.

   HINWEIS
   Wenn Sie keine dieser Tasten drücken, wird das Programm Rescue Disk nach 60 Sekunden automatisch gestartet.

Aktualisieren einer Rettungsdiskette

Es empfiehlt sich, Ihre Rettungsdiskette regelmäßig zu aktualisieren. Befolgen Sie dazu die Anweisungen zum Erstellen einer neuen Rettungsdiskette.

Automatisches Melden von Viren

Informationen zu Viren können anonym an die World Virus Map gesendet werden. Nehmen Sie das Angebot, diese kostenlose, sichere Funktion zu nutzen, an: Entweder automatisch während der Installation von VirusScan (im Dialogfeld **Informationen an Virus Map weiterleiten**) oder jederzeit auf der Registerkarte **Informationen an Virus Map weiterleiten** im Dialogfeld **VirusScan-Optionen**.

Weiterleiten von Informationen an die World Virus Map

So melden Sie Vireninformationen an die World Virus Map:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Optionen**.

   Das Dialogfeld **VirusScan-Optionen** wird geöffnet.

2 Klicken Sie auf die Registerkarte **Informationen an Virus Map weiterleiten** (Abbildung 2-14).

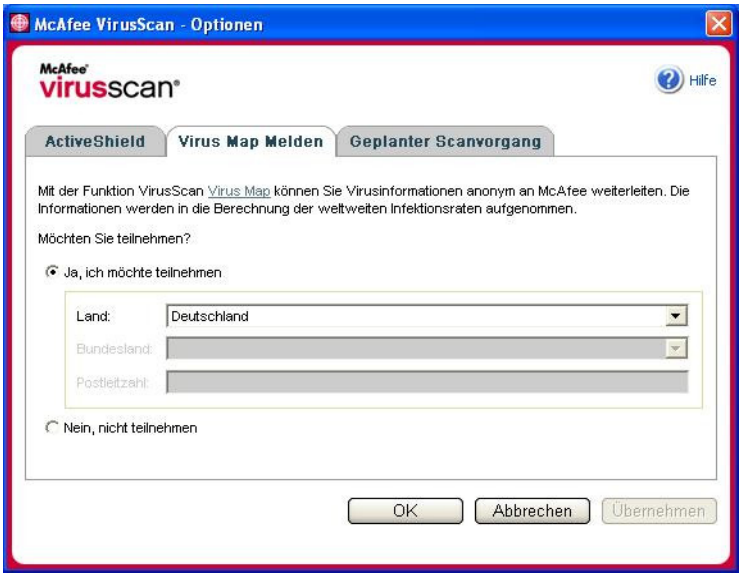


Abbildung 2-14. Optionen für die Weiterleitung von Informationen an Virus Map

3 Übernehmen Sie die Standardeinstellung **Ja, ich möchte teilnehmen**, um die Informationen anonym an McAfee zu senden. Ihre Informationen werden bei der Berechnung der weltweiten Infektionsrate in der World Virus Map berücksichtigt. Wählen Sie andernfalls **Nein, ich möchte nicht teilnehmen**. Ihre Informationen werden in diesem Falle nicht gesendet.

4 Wenn Sie in den USA leben, wählen Sie den Bundesstaat aus, und geben Sie die Postleitzahl (Zip-Code) für den Standort Ihres Computers ein. Wenn Sie nicht in den USA leben, versucht VirusScan automatisch das Land auszuwählen, in dem sich der Computer befindet.

5 Klicken Sie auf **OK**.

Anzeigen der World Virus Map

Auch wenn Sie keine Informationen an die World Virus Map senden, können Sie die neuesten globalen Infektionsraten über das McAfee-Symbol auf der Windows-Taskleiste anzeigen.

So zeigen Sie die World Virus Map an:

- Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **World Virus Map**.

Die Webseite mit der **World Virus Map** wird angezeigt (Abbildung 2-15).

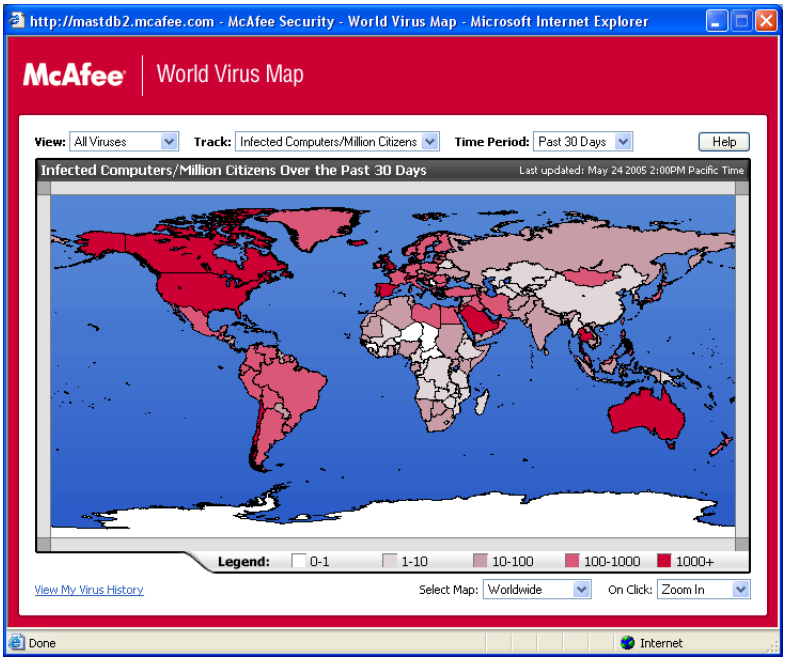

http://mastdb2.mcafee.com - McAfee Security - World Virus Map - Microsoft Internet Explorer
McAfee
World Virus Map
View: All Viruses
Track: Infected Computers/Million Citizens
Time Period: Past 30 Days
Help
Infected Computers/Million Citizens Over the Past 30 Days
Last updated: May 24 2005 2:00PM Pacific Time
Legend: 0-1 1-10 10-100 100-1000 1000+
View My Virus History
Select Map: Worldwide
On Click: Zoom In
Done
Internet

Abbildung 2-15. World Virus Map

Standardmäßig wird auf der World Virus Map die Anzahl der Computer angezeigt, die weltweit in den letzten 30 Tagen infiziert wurden. Außerdem sehen Sie, wann die gemeldeten Daten zuletzt aktualisiert wurden. Sie können die Ansicht der World Virus Map so ändern, dass die Anzahl der infizierten Dateien angezeigt wird, oder den Zeitraum modifizieren, um nur die Ergebnisse der letzten sieben Tage oder der letzten 24 Stunden anzuzeigen.

Im Abschnitt **Virus Tracking** finden Sie eine Auflistung der gesamten durchsuchten Dateien, der infizierten Dateien und der infizierten Computer, die seit dem angegebenen Datum gemeldet wurden.

Aktualisieren von VirusScan

Wenn Sie mit dem Internet verbunden sind, ermittelt VirusScan alle vier Stunden, ob Updates zur Verfügung stehen, lädt sie automatisch herunter und installiert wöchentliche Virusdefinitions-Updates, ohne Sie bei der Arbeit zu unterbrechen.

Virusdefinitionsdateien sind maximal 100 KB groß und beeinträchtigen die Systemleistung während des Downloads folglich nur geringfügig.

Bei einem Produktupdate oder Virusausbruch erhalten Sie eine entsprechende Benachrichtigung. Sie können nach der Benachrichtigung VirusScan aktualisieren, um den Ausbruch des Virus zu verhindern.

Automatisches Prüfen auf Updates

McAfee SecurityCenter ist so konfiguriert, dass alle vier Stunden automatisch nach Updates für Ihre gesamten McAfee-Dienste gesucht wird, sofern Sie mit dem Internet verbunden sind, und Sie durch Warnmeldungen und akustische Signale benachrichtigt werden. Standardmäßig lädt SecurityCenter automatisch alle verfügbaren Updates herunter und installiert sie.

HINWEIS
In einigen Fällen werden Sie aufgefordert, den Computer neu zu starten, um den Installationsvorgang für das Update abzuschließen. Speichern Sie Ihre Arbeit, und schließen Sie vor dem Neustart alle Programme.

Manuelles Prüfen auf Updates

Zusätzlich zum automatischen Suchen nach Updates, das alle vier Stunden durchgeführt wird (vorausgesetzt, eine Internetverbindung besteht), haben Sie außerdem jederzeit die Möglichkeit, manuell nach Updates zu suchen.

So suchen Sie manuell nach VirusScan-Updates:

1. Stellen Sie sicher, dass Ihr Computer mit dem Internet verbunden ist.
2. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, und klicken Sie dann auf **Updates**.

   Das Dialogfeld **SecurityCenter-Updates** wird geöffnet.
3. Klicken Sie auf **Jetzt prüfen**.

   Wenn ein Update vorhanden ist, wird das Dialogfeld **VirusScan-Updates** geöffnet (Abbildung 2-16 auf Seite 49). Klicken Sie auf **Aktualisieren**, um fortzufahren.

Wenn keine Updates verfügbar sind, werden Sie in einem Dialogfeld darüber informiert, dass VirusScan auf dem neuesten Stand ist. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

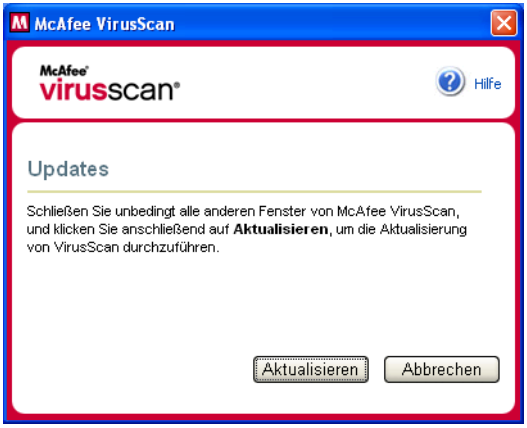


Abbildung 2-16. Dialogfeld „Updates“

4 Melden Sie sich bei der Website an, wenn Sie dazu aufgefordert werden. Das Update wird automatisch vom **Update-Assistenten** installiert.

5 Klicken Sie nach Abschluss der Update-Installation auf **Fertig stellen**.

HINWEIS
In einigen Fällen werden Sie aufgefordert, den Computer neu zu starten, um den Installationsvorgang für das Update abzuschließen. Speichern Sie Ihre Arbeit, und schließen Sie vor dem Neustart alle Programme.

McAfee Personal Firewall Plus 3

Willkommen bei McAfee Personal Firewall Plus.

McAfee Personal Firewall Plus-Software bietet erweiterten Schutz für Ihren Computer und Ihre persönlichen Daten. Personal Firewall baut eine Barriere zwischen Ihrem Computer und dem Internet auf. Dabei wird der Internetverkehr im Hintergrund auf verdächtige Aktivitäten hin überwacht.

Das Programm umfasst folgende Funktionen:

- Abwehr von potentiellen Hacker-Angriffen
- Ergänzung von Antivirus-Software
- Überwachung von Internet- und Netzwerkaktivitäten
- Warnungen bei potentiell schädlichen Ereignissen
- Bereitstellung detaillierter Informationen zu verdächtigem Internetverkehr
- Integration der Funktionalität von HackerWatch.org, einschließlich Ereignismeldung, selbsttestende Tools und die Möglichkeit, gemeldete Ereignisse per E-Mail an andere Online-Behörden zu senden.
- Bereitstellung detaillierter Funktionen zur Verfolgung und Ereignisrecherche

Neue Funktionen

- **Verbesserter Schutz bei Spielen**
  McAfee Personal Firewall Plus schützt Ihren Computer vor versuchtem Eindringen und vor verdächtigen Aktivitäten, während Sie Spiele im Vollbildmodus spielen. Die Warnungen können jedoch auch ausgeblendet werden, wenn ein versuchtes Eindringen oder verdächtige Aktivitäten entdeckt wurden. Nachdem Sie das Spiel beendet haben, werden rote Warnmeldungen angezeigt.

- **Verbesserte Zugriffsverwaltung**
  Mit McAfee Personal Firewall Plus können Sie auf dynamische Art und Weise Anwendungen vorübergehend Zugriff auf das Internet ermöglichen. Der Anwendung wird der Zugriff nur solange gewährt, bis sie wieder geschlossen wird. Entdeckt Personal Firewall ein unbekanntes Programm, das versucht, mit dem Internet zu kommunizieren, erhalten Sie über eine rote Warnung die Möglichkeit, der Anwendung vorübergehend Zugriff auf das Internet zu gewähren.

- **Umfassendere Sicherheitsprüfung**
  Mithilfe des Sperrmodus in McAfee Personal Firewall Plus können Sie den gesamten eingehenden und ausgehenden Internetverkehr zwischen Ihrem Computer und dem Internet sofort sperren. Sie können den Sperrmodus in Personal Firewall auf drei verschiedene Arten aktivieren und deaktivieren.

- **Verbesserte Optionen für die Wiederherstellung**
  Mit den Wiederherstellungsoptionen können Sie bei Personal Firewall automatisch die Standardeinstellungen wiederherstellen. Wenn Personal Firewall ein nicht gewünschtes Verhalten aufweist, das Sie nicht korrigieren können, können Sie die aktuellen Einstellungen rückgängig machen und die Standardeinstellungen des Produkts wiederherstellen.

- **Schutz für die Internetverbindung**
  Damit ein Benutzer nicht versehentlich die Internetverbindung deaktiviert, wird bei einer blauen Warnung die Option zum Sperren der Internetadresse nicht angezeigt, wenn Personal Firewall erkannt hat, dass die Internetverbindung von einem DHCP- oder DNS-Server hergestellt wurde. Wenn der eingehende Datenverkehr nicht von einem DHCP- oder DNS-Server stammt, wird die Option angezeigt.

- **Verbesserte HackerWatch.org-Integration**
  Das Melden potentieller Hacker ist einfacher denn je. McAfee Personal Firewall Plus verbessert die Funktionalität von HackerWatch.org. Dies beinhaltet die Übermittlung von potentiell gefährlichen Ereignissen an die Datenbank.

- **Erweiterter intelligenter Umgang mit Anwendungen**
  Wenn eine Anwendung Internetzugriff anfordert, prüft Personal Firewall zuerst, ob es die Anwendung als vertrauenswürdig oder bösartig einstuft. Gilt die Anwendung als vertrauenswürdig, gewährt Personal Firewall ihr automatisch den Zugriff auf das Internet, ohne dass weitere Aktionen erforderlich wären.

- **Erweiterte Erkennung trojanischer Pferde**
  Personal Firewall vereint die Anwendungsverbindungsverwaltung mit einer erweiterten Datenbank, um mehr potentiell bösartige Anwendungen, beispielsweise trojanische Pferde, erkennen und blockieren zu können und somit daran zu hindern, auf das Internet zuzugreifen und möglicherweise Ihre persönlichen Daten weiterzugeben.

- **Verbesserte visuelle Verfolgung**
  Visual Trace bietet leicht verständliche grafische Darstellungen, in denen die Quelle der feindlichen Angriffe und des weltweiten Datenverkehrs einschließlich detaillierter Kontakt- bzw. Benutzerinformationen zu den Quell-IP-Adressen angezeigt werden.

- **Noch benutzerfreundlicher**
  McAfee Personal Firewall enthält einen Setup-Assistenten sowie ein User Tutorial, die Benutzer bei Einrichtung und Verwendung der Firewall unterstützen. Obwohl das Produkt zur Verwendung ohne Benutzereingriff entwickelt wurde, stellt McAfee den Benutzern zahlreiche Ressourcen zur Verfügung, um ihnen das Verständnis der Firewall zu erleichtern und deren Nutzen zu verdeutlichen.

- **Erweiterte Eindringungserkennung**
  Das Eindringungserkennungssystem (Intrusion Detection System, IDS) von Personal Firewall erkennt gängige Angriffstypen sowie andere verdächtige Aktivitäten. Die Eindringungserkennung prüft jedes Datenpaket auf verdächtige Datenübertragungen oder Übertragungsmethoden und speichert diese im Ereignisprotokoll.

- **Verbesserte Datenverkehrsanalyse**
  McAfee Personal Firewall Plus ermöglicht es Benutzern, eingehende und ausgehende Daten des Computers anzuzeigen. Darüber hinaus können Anwendungsverbindungen sowie Anwendungen, die aktiv nach offenen Verbindungen suchen, angezeigt werden. So können Benutzer Anwendungen, die möglicherweise anfällig für Eindringlinge sind, erkennen und entsprechend reagieren.

Entfernen anderer Firewalls

Bevor Sie die McAfee Personal Firewall Plus-Software installieren, müssen Sie alle anderen Firewall-Programme auf Ihrem Computer entfernen. Befolgen Sie hierzu die Deinstallationsanweisungen zu Ihrem Firewall-Programm.

HINWEIS
Wenn Sie Windows XP verwenden, müssen Sie die integrierte Firewall vor der Installation von McAfee Personal Firewall Plus nicht zwingend deaktivieren. Wir empfehlen jedoch, die integrierte Firewall dennoch zu deaktivieren. Anderenfalls erhalten Sie keine Ereignismeldungen im Protokoll für eingehende Ereignisse in McAfee Personal Firewall Plus.

Festlegen der Standard-Firewall

McAfee Personal Firewall kann Berechtigungen und Datenverkehr für Internetanwendungen auf Ihrem Computer auch dann verwalten, wenn erkannt wird, dass die Windows-Firewall auf Ihrem System ausgeführt wird.

Bei der Installation deaktiviert McAfee Personal Firewall automatisch die Windows-Firewall und richtet sich selbsttätig als standardmäßige Firewall ein. Die gesamte Firewall-Funktionalität und diesbezügliche Meldungen kommen anschließend von McAfee Personal Firewall. Wenn Sie später die Windows-Firewall über das Windows-Sicherheitscenter oder die Windows-Systemsteuerung aktivieren und auf Ihrem Computer beide Firewalls ausführen sollten, kann die Protokollfunktion in McAfee Firewall teilweise verloren gehen, während Status- und Warnmeldungen möglicherweise doppelt angezeigt werden.

HINWEIS

Wenn beide Firewalls aktiviert sind, zeigt McAfee Personal Firewall nicht alle blockierten IP-Adressen auf der Registerkarte der eingehenden Ereignisse an. Die Windows-Firewall fängt die meisten dieser Ereignisse ab und blockiert sie, wodurch ihre Erkennung und Protokollierung durch McAfee Personal Firewall unterbunden wird. McAfee Personal Firewall kann jedoch auf der Basis anderer Sicherheitsfaktoren zusätzlichen Datenverkehr blockieren. Diese Ereignisse werden protokolliert.

Die Protokollierung ist in der Windows-Firewall standardmäßig deaktiviert. Wenn Sie jedoch beide Firewalls verwenden möchten, können Sie die Windows-Firewall-Protokollfunktion aktivieren. Das Standardprotokoll der Windows-Firewall ist C:\Windows\pfirewall.log.

Um sicherzustellen, dass Ihr Computer von mindestens einer Firewall geschützt wird, wird die Windows-Firewall automatisch erneut aktiviert, sobald McAfee Personal Firewall deinstalliert wird.

Wenn Sie McAfee Personal Firewall deaktivieren oder die Sicherheitseinstellung des Programms auf **Offen** setzen, ohne die Windows-Firewall manuell zu aktivieren, wird der gesamte Firewall-Schutz, mit Ausnahme der zuvor bereits blockierten Anwendungen, entfernt.

Festlegen der Sicherheitsstufe

Anhand von Sicherheitsoptionen können Sie festlegen, wie Personal Firewall reagieren soll, wenn unerwünschter Datenverkehr erkannt wird. Standardmäßig ist die Sicherheitsstufe **Standardsicherheit** aktiviert. Wenn bei Verwendung der Sicherheitsstufe **Standardsicherheit** eine Anwendung Internetzugriff anfordert und Sie der Anforderung nachkommen, gewähren Sie damit Vollzugriff. Vollzugriff ermöglicht der Anwendung das Senden und Empfangen unaufgeforderter Daten auf Nicht-Systemanschlüssen.

So konfigurieren Sie Sicherheitseinstellungen:

1. Klicken Sie in der Windows-Taskleiste mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und wählen Sie **Optionen** aus.
2. Klicken Sie auf das Symbol **Sicherheitseinstellungen**.
3. Legen Sie die Sicherheitsstufe fest, indem Sie den Schieberegler in die gewünschte Position bringen.

   Die Sicherheitsstufen rangieren von „Verbindung schließen“ bis „Offen (Kein Filter)“:

   - **Verbindung schließen:** Alle Internetverbindungen Ihres Computers werden geschlossen. Sie können diese Einstellung verwenden, um Anschlüsse zu blockieren, die Sie auf der Seite „Systemdienste“ als offen konfiguriert haben.
   - **Eingeschränkte Sicherheit:** Wenn eine Anwendung eine bestimmte Form des Internetzugriffs erfordert (z. B. „Nur ausgehender Zugriff“), können Sie die Internetverbindung für diese Anwendung zulassen oder blockieren. Wenn eine Anwendung später Vollzugriff anfordert, können Sie entweder Vollzugriff gewähren oder den Zugriff auf den ausgehenden Datenverkehr beschränkt belassen.
   - **Standardsicherheit (empfohlen):** Wenn eine Anwendung Internetzugriff anfordert und Sie der Anforderung nachkommen, erhält die Anwendung damit Vollzugriff für eingehenden und ausgehenden Datenverkehr.
   - **Vertrauenswürdige Sicherheit:** Allen Anwendungen wird automatisch vertraut, sobald sie versuchen, auf das Internet zuzugreifen. Sie können Personal Firewall jedoch so konfigurieren, dass Sie durch Warnungen über neue Anwendungen auf Ihrem Computer informiert werden. Verwenden Sie diese Einstellung, wenn Sie bemerken, dass bestimmte Spiele oder Streaming Media nicht funktionieren.
   - **Offen (Kein Filter):** Ihre Firewall ist deaktiviert. Diese Einstellung lässt den gesamten Datenverkehr ohne Filterung durch Personal Firewall passieren.

     HINWEIS
     Zuvor blockierte Anwendungen werden auch weiterhin blockiert, wenn die Sicherheitseinstellung der Firewall auf **Offen (Kein Filter)** oder **Verbindung schließen** gesetzt wird. Wenn dies nicht erwünscht ist, können Sie entweder die Berechtigungen der Anwendung auf **Vollzugriff zulassen** setzen oder die Berechtigungsregel **Blockiert** aus der Liste **Internetanwendungen** löschen.

4 Wählen Sie zusätzliche Sicherheitseinstellungen aus:

HINWEIS
Wenn auf Ihrem Computer Windows XP ausgeführt wird und mehrere XP-Benutzer hinzugefügt wurden, stehen diese Optionen nur dann zur Verfügung, wenn Sie auf Ihrem Computer als Administrator angemeldet sind.

- **Ereignisse der Eindringungserkennung im Protokoll der eingehenden Ereignisse aufzeichnen:** Wenn Sie diese Option auswählen, werden die von IDS erkannten Ereignisse im Protokoll eingehender Ereignisse angezeigt. Das Eindringungserkennungssystem (Intrusion Detection System, IDS) erkennt gängige Angriffstypen sowie andere verdächtige Aktivitäten. Die Eindringungserkennung prüft jedes eingehende und ausgehende Datenpaket auf verdächtige Datenübertragungen oder Übertragungsmethoden. Die Pakete werden mit einer Signaturdatenbank verglichen und automatisch verworfen, wenn sie von dem „schuldigen" Computer kommen.

  IDS sucht nach bestimmten von Angreifern verwendeten Verkehrsmustern. Jedes von Ihrem Computer empfangene Datenpaket wird von IDS überprüft, um verdächtigen Datenverkehr oder Datenverkehr, der bekannten Angriffen gleicht, zu erkennen. Wenn Personal Firewall beispielsweise ICMP-Pakete erkennt, prüft es diese Pakete auf verdächtige Verkehrsmuster, indem es den ICMP-Datenverkehr mit den Mustern bekannter Angriffe vergleicht.

- **ICMP-Ping-Anforderungen akzeptieren:** ICMP-Datenverkehr wird hauptsächlich für Ablaufverfolgungen und Ping-Signale verwendet. Ping-Signale wiederum dienen häufig zur Durchführung von kurzen Tests, bevor versucht wird, eine Kommunikation zu initiieren. Wenn Sie ein Peer-to-Peer-Dateifreigabeprogramm verwenden oder verwendet haben, erhalten Sie möglicherweise eine große Anzahl von Ping-Signalen. Wenn Sie diese Option auswählen, lässt Personal Firewall alle Ping-Anforderungen zu, ohne die Ping-Signale im Protokoll der eingehenden Ereignisse aufzuzeichnen. Wenn Sie die Option nicht auswählen, blockiert Personal Firewall alle Ping-Anforderungen und zeichnet die Ping-Signale im Protokoll der eingehenden Ereignisse auf.

- **Änderung der Personal Firewall-Einstellungen für eine eingeschränkte Anzahl an Benutzern zulassen:** Wenn auf Ihrem Computer Windows XP oder Windows 2000 Professional mit mehreren Benutzern ausgeführt wird, wählen Sie diese Option aus, damit auch XP-Benutzer mit eingeschränkten Rechten die Einstellungen für Personal Firewall ändern können.

5 Klicken Sie auf **OK**, nachdem Sie die Änderungen vorgenommen haben.

Testen von McAfee Personal Firewall Plus

Sie können Ihre Personal Firewall-Installation auf mögliche Sicherheitslücken bei Eindringversuchen und verdächtigen Aktivitäten testen.

So testen Sie Ihre Personal Firewall-Installation über das McAfee-Taskleistensymbol:

- Klicken Sie mit der rechten Maustaste in der Windows-Taskleiste auf das McAfee-Symbol, und wählen Sie **Firewall testen** aus.

Personal Firewall startet Internet Explorer und zeigt auf die Website http://www.hackerwatch.org/, die von McAfee verwaltet wird. Befolgen Sie die Anweisungen auf der Testseite von HackerWatch.org, um Personal Firewall zu testen.

Info zur Zusammenfassung

Die Personal Firewall-Zusammenfassung enthält vier Zusammenfassungsseiten:

- Hauptübersicht
- Anwendungsübersicht
- Ereignisübersicht
- HackerWatch-Zusammenfassung

Die Zusammenfassungsseiten enthalten unterschiedliche Berichte zu den letzten eingegangenen Ereignissen, dem Anwendungsstatus sowie der von HackerWatch.org gemeldeten weltweiten Eindringaktivität. Außerdem finden Sie hier Links zu Tasks, die in Personal Firewall häufig ausgeführt werden.

So öffnen Sie die Hauptübersicht in Personal Firewall:

- Klicken Sie mit der rechten Maustaste in der Windows-Taskleiste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und wählen Sie anschließend **Zusammenfassung anzeigen** (Abbildung 3-1) aus.

Abbildung 3-1. Hauptübersicht

Klicken Sie auf die folgenden Steuerelemente, um zu den verschiedenen Zusammenfassungen zu navigieren:

Objekt	Beschreibung
Ansicht ändern	Klicken Sie auf **Ansicht ändern**, um eine Zusammenfassungsliste zu öffnen. Von dieser Liste aus können Sie die gewünschte Zusammenfassung zur Ansicht auswählen.
Pfeil nach rechts	Klicken Sie auf den Pfeil nach rechts, um die nächste Zusammenfassung anzuzeigen.
Pfeil nach links	Klicken Sie auf den Pfeil nach links, um die vorherige Zusammenfassung anzuzeigen.
Home	Klicken Sie auf das Home-Symbol, um zur **Hauptübersicht** zurückzukehren.

Die Seite mit der Hauptübersicht enthält folgende Informationen:

Objekt	Beschreibung
Sicherheitseinstellung	Aus dem Status der Sicherheitseinstellung geht hervor, auf welche Sicherheitsstufe die Firewall eingestellt ist. Klicken Sie auf den Link, um die Sicherheitsstufe zu ändern.
Blockierte Ereignisse	Hier wird die Anzahl der Ereignisse angezeigt, die am aktuellen Tag blockiert wurden. Klicken Sie auf den Link, um Ereignisdetails von der Seite der eingehenden Ereignisse anzuzeigen.
Änderungen von Anwendungsregeln	Hier wird die Anzahl der Anwendungsregeln angezeigt, die in letzter Zeit geändert wurden. Klicken Sie auf den Link, um die Liste der zugelassenen und blockierten Anwendungen anzuzeigen und Anwendungsberechtigungen zu ändern.
Neues	Unter **Neues** wird die Anwendung angezeigt, der zuletzt uneingeschränkter Zugriff auf das Internet gewährt wurde.
Letztes Ereignis	Unter **Letztes Ereignis** werden die letzten eingehenden Ereignisse angezeigt. Klicken Sie auf einen Link, um den Ablauf des betreffenden Ereignisses zu verfolgen oder die IP-Adresse als vertrauenswürdig einzustufen. Wenn Sie einer IP-Adresse vertrauen, wird der Empfang von Datenverkehr von dieser IP-Adresse auf Ihrem Computer ermöglicht.
Täglicher Bericht	Unter **Täglicher Bericht** wird die Anzahl der eingehenden Ereignisse angezeigt, die von Personal Firewall am aktuellen Tag, in der aktuellen Woche oder im aktuellen Monat blockiert wurden. Klicken Sie auf den Link, um Ereignisdetails von der Seite der eingehenden Ereignisse anzuzeigen.
Aktive Anwendungen	Unter **Aktive Anwendungen** werden die Anwendungen aufgeführt, die zurzeit auf Ihrem Computer ausgeführt werden und auf das Internet zugreifen. Klicken Sie auf eine Anwendung, um anzuzeigen, mit welchen IP-Adressen die Anwendung eine Verbindung herstellt.
Häufige Tasks	Klicken Sie auf einen Link unter **Häufige Tasks**, um auf Personal Firewall-Seiten die Aktivitäten der Firewall anzuzeigen bzw. Tasks durchzuführen.

So öffnen Sie die Seite „Anwendungsübersicht“:

1 Klicken Sie in der Windows-Taskleiste mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und wählen Sie anschließend **Zusammenfassung anzeigen** aus.

2 Klicken Sie auf **Ansicht ändern** und wählen dann **Anwendungsübersicht** aus.

Diese Seite enthält die folgenden Informationen:

Objekt	Beschreibung
Datenverkehrsmonitor	Der **Datenverkehrsmonitor** zeigt eingehende und ausgehende Internetverbindungen der vergangenen 15 Minuten. Klicken Sie auf das Diagramm, um Details zum Datenverkehr anzuzeigen.
Aktive Anwendungen	Unter **Aktive Anwendungen** wird die Bandbreitennutzung der aktivsten Anwendungen des Computers in den letzten 24 Stunden angegeben. **Anwendung**: Die Anwendung, die auf das Internet zugreift. **%**: Der Prozentsatz der Bandbreite, der von der Anwendung genutzt wird. **Berechtigung**: Die Art von Internetzugriff, die für die Anwendung zulässig ist. **Regel erstellt am**: Der Zeitpunkt, zu dem die Anwendungsregel erstellt wurde.
Neues	Unter **Neues** wird die Anwendung angezeigt, der zuletzt uneingeschränkter Zugriff auf das Internet gewährt wurde.
Aktive Anwendungen	Unter **Aktive Anwendungen** werden die Anwendungen aufgeführt, die zurzeit auf Ihrem Computer ausgeführt werden und auf das Internet zugreifen. Klicken Sie auf eine Anwendung, um anzuzeigen, mit welchen IP-Adressen die Anwendung eine Verbindung herstellt.
Häufige Tasks	Klicken Sie auf einen Link unter **Häufige Tasks**, um auf Personal Firewall-Seiten den Anwendungsstatus anzuzeigen bzw. anwendungsbezogene Tasks durchzuführen.

So öffnen Sie die Seite „Ereignisübersicht“:

1 Klicken Sie in der Windows-Taskleiste mit der rechten Maustaste auf das McAfee-Symbol , zeigen Sie auf **Personal Firewall**, und wählen Sie anschließend **Zusammenfassung anzeigen** aus.

2 Klicken Sie auf **Ansicht ändern**, und wählen Sie dann **Ereignisübersicht** aus.

Diese Seite enthält die folgenden Informationen:

Objekt	Beschreibung
Anschlussvergleich	Unter **Anschlussvergleich** wird ein Kreisdiagramm der Anschlüsse auf Ihrem Computer angezeigt, auf die in den letzten 30 Tagen am häufigsten versucht wurde zuzugreifen. Sie können auf einen Anschlussnamen klicken, um auf der Seite der eingehenden Ereignisse aufgeführte Details dazu anzuzeigen. Außerdem können Sie eine Beschreibung des Anschlusses anzeigen, indem Sie den Mauszeiger über die Anschlussnummer bewegen.
Hauptverursacher	**Hauptverursacher** zeigt die am häufigsten blockierten IP-Adressen und für jede Adresse den Zeitpunkt des letzten eingehenden Ereignisses sowie die Gesamtzahl der eingehenden Ereignisse pro Adresse in den letzten dreißig Tagen. Klicken Sie auf ein Ereignis, um Ereignisdetails von der Seite der eingehenden Ereignisse anzuzeigen.
Täglicher Bericht	Unter **Täglicher Bericht** wird die Anzahl der eingehenden Ereignisse angezeigt, die von Personal Firewall am aktuellen Tag, in der aktuellen Woche oder im aktuellen Monat blockiert wurden. Klicken Sie auf eine Zahl, um Ereignisdetails aus dem Protokoll der eingehenden Ereignisse anzuzeigen.
Letztes Ereignis	Unter **Letztes Ereignis** werden die letzten eingehenden Ereignisse angezeigt. Klicken Sie auf einen Link, um den Ablauf des betreffenden Ereignisses zu verfolgen oder die IP-Adresse als vertrauenswürdig einzustufen. Wenn Sie einer IP-Adresse vertrauen, wird der Empfang von Datenverkehr von dieser IP-Adresse auf Ihrem Computer ermöglicht.
Häufige Tasks	Klicken Sie auf einen Link unter **Häufige Tasks**, um auf den Personal Firewall-Seiten Details zu Ereignissen anzuzeigen bzw. ereignisbezogene Tasks durchzuführen.

So öffnen Sie die Seite „HackerWatch-Zusammenfassung“:

1. Klicken Sie in der Windows-Taskleiste mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und wählen Sie anschließend **Zusammenfassung anzeigen** aus.
2. Klicken Sie auf **Ansicht ändern**, und wählen Sie anschließend **HackerWatch-Zusammenfassung** aus.

Diese Seite enthält die folgenden Informationen:

Objekt	Beschreibung
Weltweite Aktivität	Unter **Weltweite Aktivität** wird auf einer Weltkarte die letzte blockierte Aktivität angezeigt, die von HackerWatch.org überwacht wird. Klicken Sie auf die Karte, um die Karte von HackerWatch.org zu öffnen, auf der die globale Bedrohung analysiert wird.
Ereignisverfolgung	Unter **Ereignisverfolgung** wird die Anzahl der eingehenden Ereignisse angegeben, die an HackerWatch.org übermittelt wurden.
Globale Anschlussaktivität	Unter **Globale Anschlussaktivität** werden die Anschlüsse angegeben, die innerhalb der letzten fünf Tage offensichtlich am häufigsten eine Bedrohung dargestellt haben. Klicken Sie auf einen Anschluss, um die Anschlussnummer und -beschreibung anzuzeigen.
Häufige Tasks	Klicken Sie unter **Häufige Tasks** auf einen Link, um zu den HackerWatch.org-Seiten zu gelangen, auf denen Sie ausführlichere Informationen zur weltweiten Hackeraktivität erhalten.

Info zur Seite „Internetanwendungen“

Mithilfe der Seite „Internetanwendungen“ können Sie die Liste der zugelassenen und blockierten Anwendungen anzeigen:

So starten Sie die Seite mit den Internetanwendungen:

- Klicken Sie in der Windows-Taskleiste mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und wählen Sie anschließend **Anwendungen** (Abbildung 3-2) aus.

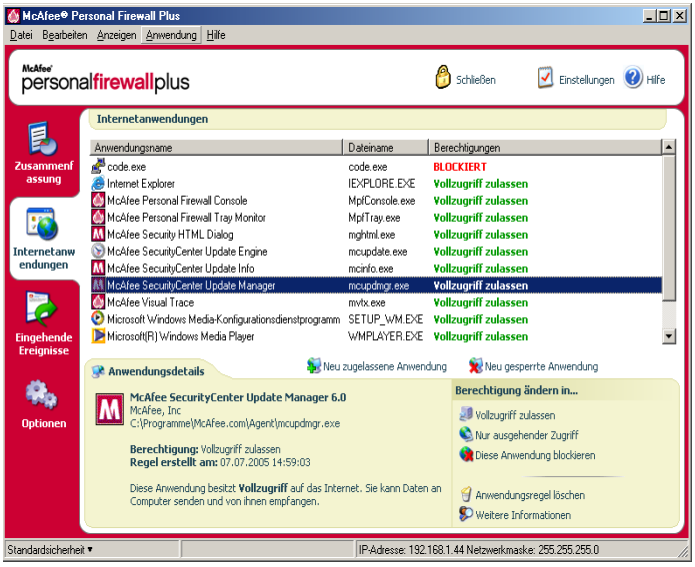


Abbildung 3-2. Seite „Internetanwendungen“

Diese Seite enthält folgende Informationen:

- Anwendungsname
- Dateinamen
- Aktuelle Berechtigungsstufen
- Anwendungsdetails: Anwendungsname und -version, Name des Unternehmens, Pfadname, Berechtigung, Zeitstempel und Erläuterungen der Berechtigungsarten.

Ändern von Anwendungsregeln

Mit Personal Firewall können Sie die Zugriffsregeln für Anwendungen ändern.

So ändern Sie eine Anwendungsregel:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und wählen Sie dann **Internetanwendungen** aus.
2. In der Liste der **Internetanwendungen** klicken Sie mit der rechten Maustaste auf die Anwendungsregel einer Anwendung und wählen eine andere Zugriffsstufe aus:
   - **Vollzugriff zulassen:** Lässt eingehende und ausgehende Internetverbindungen für die Anwendung zu.
   - **Nur ausgehender Zugriff:** Lässt nur ausgehende Internetverbindungen für die Anwendung zu.
   - **Diese Anwendung blockieren:** Lässt für diese Anwendung keinerlei Internetzugriff zu.

     HINWEIS
     Zuvor blockierte Anwendungen werden auch weiterhin blockiert, wenn für die Firewall die Sicherheitseinstellung **Offen (Kein Filter)** oder **Verbindung schließen** festgelegt wurde. Um dies zu verhindern, können Sie die entweder die Zugriffsregel der Anwendung auf **Vollzugriff zulassen** setzen oder die Berechtigungsregel **Blockiert** in der Liste **Internetanwendungen** löschen.

So löschen Sie eine Anwendungsregel:

1. Klicken Sie mit der rechten Maustaste in der Windows-Taskleiste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und wählen Sie anschließend **Internetanwendungen** aus.
2. In der Liste der **Internetanwendungen** klicken Sie mit der rechten Maustaste auf die Anwendungsregel, und wählen Sie dann **Anwendungsregel löschen** aus.

Wenn die Anwendung das nächste Mal Internetzugriff anfordert, können Sie ihre Berechtigungsstufe erneut festlegen, um sie der Liste wieder hinzuzufügen.

Zulassen und Blockieren von Internetanwendungen

So ändern Sie die Liste der zugelassenen und blockierten Internetanwendungen:

1. Klicken Sie mit der rechten Maustaste in der Windows-Taskleiste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und wählen Sie anschließend **Internetanwendungen** aus.

2 Auf der Seite mit den Internetanwendungen klicken Sie auf eine der folgenden Optionen:

- **Neu zugelassene Anwendung**: Hiermit gewähren Sie einer Anwendung vollen Internetzugriff.
- **Neu gesperrte Anwendung**: Hiermit sperren Sie den Internetzugriff einer Anwendung.
- **Anwendungsregel löschen**: Hiermit entfernen Sie eine Anwendungsregel.

Info zur Seite Eingehende Ereignisse

Über die Seite für eingehende Ereignisse können Sie das Protokoll eingehender Ereignisse anzeigen, das erstellt wird, wenn Personal Firewall unaufgeforderte Internetverbindungen blockiert.

So starten Sie die Seite „Eingehende Ereignisse“:

- Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie anschließend **Eingehende Ereignisse** (Abbildung 3-3) aus.

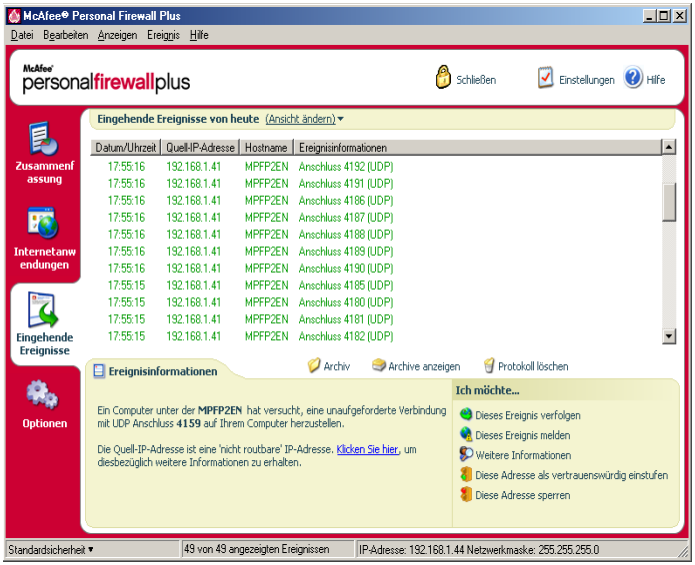

McAfee® Personal Firewall Plus
Datei Bearbeiten Anzeigen Ereignis Hilfe
personalfirewallplus
Schließen
Einstellungen
Hilfe
Zusammenfassung
Internetanwendungen
Eingehende Ereignisse
Optionen
Eingehende Ereignisse von heute (Ansicht ändern)
Datum/Uhrzeit | Quell-IP-Adresse | Hostname | Ereignisinformationen
17:55:16 192.168.1.41 MPFP2EN Anschluss 4192 (UDP)
17:55:16 192.168.1.41 MPFP2EN Anschluss 4191 (UDP)
17:55:16 192.168.1.41 MPFP2EN Anschluss 4186 (UDP)
17:55:16 192.168.1.41 MPFP2EN Anschluss 4187 (UDP)
17:55:16 192.168.1.41 MPFP2EN Anschluss 4188 (UDP)
17:55:16 192.168.1.41 MPFP2EN Anschluss 4189 (UDP)
17:55:16 192.168.1.41 MPFP2EN Anschluss 4190 (UDP)
17:55:15 192.168.1.41 MPFP2EN Anschluss 4185 (UDP)
17:55:15 192.168.1.41 MPFP2EN Anschluss 4180 (UDP)
17:55:15 192.168.1.41 MPFP2EN Anschluss 4181 (UDP)
17:55:15 192.168.1.41 MPFP2EN Anschluss 4182 (UDP)
Ereignisinformationen
Archiv
Archive anzeigen
Protokoll löschen
Ein Computer unter der MPFP2EN hat versucht, eine unaufgeforderte Verbindung mit UDP Anschluss 4159 auf Ihrem Computer herzustellen.
Die Quell-IP-Adresse ist eine 'nicht routbare' IP-Adresse. Klicken Sie hier, um diesbezüglich weitere Informationen zu erhalten.
Ich möchte...
Dieses Ereignis verfolgen
Dieses Ereignis melden
Weitere Informationen
Diese Adresse als vertrauenswürdig einstufen
Diese Adresse sperren
Standardsicherheit
49 von 49 angezeigten Ereignissen
IP-Adresse: 192.168.1.44 Netzwerkmaske: 255.255.255.0

Abbildung 3-3. Seite „Eingehende Ereignisse“

Die Seite mit den eingehenden Ereignissen enthält folgende Informationen:

- Zeitstempel
- Quell-IP-Adressen
- Hostnamen

- Dienst- oder Anwendungsnamen
- Ereignisdetails: Verbindungstypen, Verbindungsanschlüsse, Hostnamen oder IP-Adresse und Erläuterungen zu Anschlussereignissen

Erläuterungen zu Ereignissen

Info zu IP-Adressen

IP-Adressen bestehen aus Zahlen, genauer gesagt, aus vier verschiedenen Zahlenblöcken zwischen 0 und 255. Diese Zahlen identifizieren einen bestimmten Ort, an den der Datenverkehr im Internet weitergeleitet werden kann.

IP-Adresstypen

Einige IP-Adressen sind aus unterschiedlichen Gründen ungewöhnlich:

Nicht routbare IP-Adressen: Diese stellen einen privaten IP-Adressraum dar. Diese IP-Adressen können im Internet nicht verwendet werden. Private IP-Blöcke sind 10.x.x.x, 172.16.x.x bis 172.31.x.x und 192.168.x.x.

Loopback-IP-Adressen: Loopback-Adressen werden zu Testzwecken verwendet. Datenverkehr, der an diesen IP-Adressblock gesendet wird, kehrt sofort wieder zu dem Gerät zurück, von dem das Paket generiert wurde. Da das Gerät niemals verlassen wird, werden diese Adressen hauptsächlich für Hardware- und Softwaretests verwendet. Der Loopback-IP-Block lautet 127.x.x.x.

Null-IP-Adresse: Dies ist eine ungültige Adresse. Wird dieser Adresstyp erkannt, weist Personal Firewall darauf hin, dass der Datenverkehr eine leere IP-Adresse verwendet hat. Häufig ist dies ein Hinweis darauf, dass der Absender absichtlich die Quelle des Datenverkehrs verschleiert. Der Absender kann keine Antwort auf den Datenverkehr erhalten, es sei denn, das Paket geht bei einer Anwendung ein, die den Paketinhalt, d. h., die anwendungsspezifischen Anweisungen, erkennt. Jede Adresse, die mit 0 (0.x.x.x) beginnt, ist eine Null-Adresse. Beispielsweise ist 0.0.0.0 eine Null-IP-Adresse.

Ereignisse von 0.0.0.0

Wenn Ereignisse mit der IP-Adresse 0.0.0.0 angezeigt werden, gibt es hierfür zwei mögliche Ursachen. Die erste und häufigste Ursache besteht darin, dass Ihr Computer ein fehlerhaftes Paket erhalten hat. Das Internet ist nicht zu 100 % zuverlässig, und es ist immer möglich, dass fehlerhafte Pakete eingehen. Da Personal Firewall die Pakete vor der TCP/IP-Überprüfung erkennt, kann es passieren, dass diese Pakete als Ereignis gemeldet werden.

Die zweite Ursache besteht darin, dass die Quell-IP-Adresse gefälscht wurde. Gefälschte Pakete können ein Anzeichen dafür sein, dass jemand Ihren Computer auf Trojaner überprüft. Personal Firewall blockiert diese Aktivitäten, so dass Ihr Computer geschützt ist.

Ereignisse von 127.0.0.1

Ereignisse geben manchmal die Quell-IP-Adresse 127.0.0.1 an. Dies wird als Loopback-Adresse oder „localhost“ bezeichnet.

Viele legitime Programme verwenden die Loopback-Adresse für die Kommunikation zwischen Komponenten. Sie können beispielsweise viele persönliche E-Mail- oder Webserver über eine Weboberfläche konfigurieren. Um die Oberfläche aufzurufen, geben Sie „http://localhost/“ in Ihren Webbrowser ein.

Personal Firewall lässt Datenverkehr von diesen Programmen zu. Wenn also Ereignisse mit der IP-Adresse 127.0.0.1 angezeigt werden, bedeutet dies in der Regel, dass die Quell-IP-Adresse gefälscht ist. Gefälschte Pakete weisen meistens darauf hin, dass Ihr Computer von einem anderen auf Trojaner überprüft wird. Da Personal Firewall dieses versuchte Eindringen blockiert, ist Ihr Computer geschützt.

Für einige Programme, insbesondere Netscape ab Version 6.2, gilt jedoch, dass die Adresse 127.0.0.1 in die Liste der vertrauenswürdigen IP-Adressen aufgenommen werden muss. Die Komponenten dieser Programme kommunizieren so miteinander, dass Personal Firewall nicht ermitteln kann, ob es sich um lokalen Datenverkehr handelt oder nicht.

Für das Beispiel Netscape 6.2 gilt: Wenn Sie die Adresse 127.0.0.1 nicht als vertrauenswürdig einstufen, können Sie Ihre Buddyliste nicht verwenden. Wenn Sie folglich Datenverkehr von 127.0.0.1 bemerken und alle Anwendungen auf Ihrem Computer normal funktionieren, können Sie diesen Datenverkehr bedenkenlos blockieren. Wenn jedoch bei einem Programm (wie Netscape) Probleme auftreten, fügen Sie 127.0.0.1 zur Liste der vertrauenswürdigen IP-Adressen in Personal Firewall hinzu.

Wird das Problem durch die Aufnahme von 127.0.0.1 in die Liste der vertrauenswürdigen IP-Adressen behoben, müssen Sie Ihre Entscheidungsmöglichkeiten abwägen: Wenn Sie die Adresse 127.0.0.1 als vertrauenswürdig einstufen, funktioniert zwar das Programm, es besteht jedoch die Gefahr, dass Angriffe mit gefälschten Adressen ausgeführt werden. Wenn Sie diese Adresse nicht als vertrauenswürdig einstufen, funktioniert das Programm nicht; es wird jedoch die Gefahr verringert, dass Angriffe mit gefälschten Adressen ausgeführt werden.

Ereignisse von Computern in Ihrem lokalen Netzwerk (LAN)

Ereignisse können auch von Computern in Ihrem LAN (Local Area Network) generiert werden. Um anzuzeigen, dass diese Ereignisse durch Ihr Netzwerk erzeugt werden, werden sie in Personal Firewall grün dargestellt.

In der Regel empfiehlt es sich für die Einstellungen eines Unternehmens-LANs, im Dialogfeld **Vertrauenswürdige IP-Adressen** das Kontrollkästchen Alle Computer in meinem LAN als vertrauenswürdig einstufen zu aktivieren.

In einigen Situationen kann Ihr „lokales“ Netzwerk genauso gefährlich sein wie das Internet; insbesondere, wenn Ihr Computer an ein Netzwerk mit einer hohen Bandbreite, beispielsweise DSL oder Kabelmodem, angeschlossen ist. Wählen Sie in diesem Fall nicht die Option **Alle Computer in meinem LAN als vertrauenswürdig einstufen** aus. Nehmen Sie stattdessen die IP-Adressen der lokalen Computer manuell in die Liste der vertrauenswürdigen IP-Adressen auf.

Ereignisse von privaten IP-Adressen

IP-Adressen im Format 192.168.xxx.xxx, 10.xxx.xxx.xxx und 172.16.0.0 - 172.31.255.255 werden als nicht routbare oder private IP-Adressen bezeichnet. Diese IP-Adressen sollten niemals Ihr Netzwerk verlassen und können in der Regel als vertrauenswürdig angesehen werden.

Der Block 192.168.xxx.xxx wird in Zusammenhang mit Microsoft Internet Connection Sharing (ICS) verwendet. Wenn Sie ICS verwenden und Ereignisse von diesem IP-Block angezeigt werden, können Sie die IP-Adresse 192.168.255.255 in die Liste der vertrauenswürdigen IP-Adressen aufnehmen. Dadurch wird der Block 192.168.xxx.xxx als vertrauenswürdig eingestuft.

Wenn Sie nicht in einem privaten Netzwerk arbeiten und Ereignisse von diesen IP-Bereichen angezeigt werden, bedeutet dies, dass die Quell-IP-Adresse möglicherweise gefälscht ist. Gefälschte Pakete sind oft ein Zeichen dafür, dass jemand nach Trojanern sucht. Da Personal Firewall diesen Versuch blockiert hat, ist Ihr Computer sicher.

Da private IP-Adressen (je nach Netzwerk) auf unterschiedliche Computer verweisen, müssen derartige Ereignisse nicht gemeldet werden.

Anzeigen von Ereignissen im Ereignisprotokoll

Das Protokoll der eingehenden Ereignisse zeigt Ereignisse in unterschiedlicher Form an. In der Standardansicht werden nur Ereignisse des aktuellen Tags angezeigt. Sie können auch die Ereignisse anzeigen, die in der vergangenen Woche aufgetreten sind. Auch das gesamte Protokoll kann eingeblendet werden.

Des Weiteren ermöglicht Personal Firewall es Ihnen, eingehende Ereignisse von bestimmten Tagen, bestimmten Internetadressen (IP-Adressen) bzw. Ereignisse mit identischen Ereignisinformationen anzuzeigen.

Um Informationen zu einem Ereignis anzuzeigen, klicken Sie auf das Ereignis und zeigen die Informationen im Bereich **Ereignisinformationen** an.

Anzeigen der Ereignisse von heute

Verwenden Sie diese Option, um die Ereignisse des heutigen Tags anzuzeigen.

So zeigen Sie die Ereignisse von heute an:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie anschließend **Eingehende Ereignisse** aus.
2. Klicken Sie im Protokoll der eingehenden Ereignisse mit der rechten Maustaste auf ein Ereignis, und klicken Sie dann auf **Ereignisse von heute anzeigen**.

Anzeigen der Ereignisse aus dieser Woche

Verwenden Sie diese Option, um die Ereignisse dieser Woche anzuzeigen.

So zeigen Sie die Ereignisse aus dieser Woche an:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie anschließend **Eingehende Ereignisse** aus.
2. Klicken Sie im Protokoll der eingehenden Ereignisse mit der rechten Maustaste auf ein Ereignis, und klicken Sie dann auf **Ereignisse aus dieser Woche anzeigen**.

Anzeigen des vollständigen Protokolls eingehender Ereignisse

Verwenden Sie diese Option, um alle Ereignisse dieser Woche anzuzeigen.

So zeigen Sie alle Ereignisse im Protokoll eingehender Ereignisse an:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und klicken Sie auf **Eingehende Ereignisse**.
2. Klicken Sie im Protokoll der eingehenden Ereignisse mit der rechten Maustaste auf ein Ereignis, und klicken Sie dann auf **Vollständiges Protokoll anzeigen**.

   Das Protokoll der eingehenden Ereignisse zeigt alle Ereignisse an.

Anzeigen von Ereignissen eines bestimmten Tags

Verwenden Sie diese Option, um die Ereignisse eines bestimmten Tags anzuzeigen.

So zeigen Sie die Ereignisse eines bestimmten Tags an:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie anschließend **Eingehende Ereignisse** aus.
2. Klicken Sie im Protokoll der eingehenden Ereignisse mit der rechten Maustaste auf ein Ereignis, und klicken Sie dann auf **Nur Ereignisse des ausgewählten Tages anzeigen**.

Anzeigen von Ereignissen einer bestimmten Internetadresse

Verwenden Sie diese Option, um andere Ereignisse anzuzeigen, die von einer bestimmten Internetadresse stammen.

So zeigen Sie Ereignisse von einer bestimmten Internetadresse an:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und klicken Sie auf **Eingehende Ereignisse**.
2. Klicken Sie im Protokoll der eingehenden Ereignisse mit der rechten Maustaste auf ein Ereignis, und klicken Sie dann auf **Nur Ereignisse von einer bestimmten Internetadresse anzeigen**.

Anzeigen von Ereignissen, die über identische Ereignisinformationen verfügen

Verwenden Sie diese Option, wenn Sie wissen möchten, ob das Protokoll der eingehenden Ereignisse weitere Ereignisse enthält, die in der Spalte „Ereignisinformationen“ dieselben Informationen aufweisen wie das von Ihnen ausgewählte Ereignis. Sie können auf diese Weise ermitteln, wie oft dieses Ereignis stattgefunden hat, und überprüfen, ob die Ereignisse von derselben Quelle stammen. Aus der Spalte „Ereignisinformationen“ geht eine Beschreibung des Ereignisses und, falls bekannt, das gängige Programm bzw. der gängige Dienst hervor, das bzw. der diesen Anschluss verwendet.

So zeigen Sie Ereignisse an, die über identische Ereignisinformationen verfügen:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und klicken Sie auf **Eingehende Ereignisse**.
2. Klicken Sie im Protokoll der eingehenden Ereignisse mit der rechten Maustaste auf ein Ereignis, und klicken Sie dann auf **Nur Ereignisse mit identischen Ereignisinformationen anzeigen**.

Reagieren auf eingehende Ereignisse

Zusätzlich zur Überprüfung von Details zu Ereignissen im Protokoll eingehender Ereignisse können Sie eine visuelle Verfolgung der IP-Adressen zu Ereignissen im Protokoll eingehender Ereignisse durchführen oder Ereignisdetails auf der Website der Anti-Hacker-Online-Community HackerWatch.org anzeigen.

Verfolgen eines ausgewählten Ereignisses

Sie können versuchen, eine visuelle Verfolgung der IP-Adresse für ein Ereignis im Protokoll eingehender Ereignisse durchzuführen.

So verfolgen Sie ein ausgewähltes Ereignis:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie **Eingehende Ereignisse** aus.
2. Im Protokoll der eingehenden Ereignisse klicken Sie mit der rechten Maustaste auf das zu verfolgende Ereignis und klicken dann auf **Ausgewähltes Ereignis verfolgen**. Sie können auch auf ein Ereignis doppelklicken, um es zu verfolgen.

Standardmäßig beginnt Personal Firewall eine visuelle Verfolgung mithilfe des integrierten Visual Trace-Programms.

Abrufen von Ratschlägen von HackerWatch.org

So rufen Sie Ratschläge von HackerWatch.org ab:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und wählen Sie **Eingehende Ereignisse** aus.
2. Wählen Sie den Ereigniseintrag auf der Seite der eingehenden Ereignisse aus, und klicken Sie dann im Bereich **Ich möchte** auf **Weitere Informationen**.

Ihr Standard-Webbrowser wird gestartet und öffnet die Seite HackerWatch.org, um Informationen zum Ereignistyp abzurufen und zu ermitteln, ob das Ereignis gemeldet werden sollte.

Melden eines Ereignisses

Um ein Ereignis zu melden, das Ihrer Meinung nach einen Angriff auf Ihren Computer darstellte, gehen Sie folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie **Eingehende Ereignisse** aus.
2. Klicken Sie auf das zu meldende Ereignis und danach im Bereich **Ich möchte** auf **Dieses Ereignis melden**.

Personal Firewall meldet das Ereignis unter Ihrer eindeutigen ID an die Website von HackerWatch.org.

Anmelden bei HackerWatch.org

Beim ersten Öffnen der Zusammenfassung kontaktiert Personal Firewall HackerWatch.org, um Ihre eindeutige Benutzer-ID zu generieren. Wenn Sie ein eingetragener Benutzer sind, wird Ihre Anmeldung automatisch überprüft. Sind Sie ein neuer Benutzer, müssen Sie einen Benutzernamen sowie eine E-Mail-Adresse angeben und in der Bestätigungs-E-Mail von HackerWatch.org auf den Link zur Bestätigung klicken, damit Sie auf der Website die Funktionen zum Filtern und Senden von Ereignissen verwenden können.

Sie können Ereignisse auch ohne Überprüfung Ihrer Benutzer-ID an HackerWatch.org melden. Um Ereignisse zu filtern und als E-Mail an einen Freund zu senden, müssen Sie sich jedoch für den Dienst anmelden.

Durch die Anmeldung für den Dienst können wir Ihre Angaben überwachen und Sie benachrichtigen, wenn HackerWatch.org weitere Informationen oder Maßnahmen benötigt. Eine Anmeldung ist außerdem erforderlich, da wir alle eingegangenen Informationen bezüglich ihrer Nützlichkeit bestätigen müssen.

E-Mail-Adressen werden von HackerWatch.org vertraulich behandelt. Wenn ein ISP weitere Informationen anfordert, wird die Anfrage über HackerWatch.org weitergeleitet. Ihre E-Mail-Adresse wird niemals bekannt gegeben.

Einstufen einer Adresse als vertrauenswürdige Adresse

Sie können die Seite der eingehenden Ereignisse dazu verwenden, eine IP-Adresse zur Liste der vertrauenswürdigen IP-Adresse hinzuzufügen, um eine permanente Verbindung zuzulassen.

Wenn auf der Seite eingehender Ereignisse ein Ereignis angezeigt wird, das eine zuzulassende IP-Adresse enthält, können Sie festlegen, dass Personal Firewall Verbindungen mit dieser Adresse in jedem Fall ermöglicht.

So fügen Sie eine IP-Adresse zur Liste der vertrauenswürdigen IP-Adressen hinzu:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie **Eingehende Ereignisse** aus.
2. Klicken Sie mit der rechten Maustaste auf das Ereignis, dessen IP-Adresse als vertrauenswürdig eingestuft werden soll, und klicken Sie anschließend auf **Quell-IP-Adresse als vertrauenswürdig einstufen**.

Überprüfen Sie, ob die in der Bestätigungsmeldung „Diese Adresse als vertrauenswürdig einstufen“ angegebene IP-Adresse korrekt ist, und klicken Sie anschließend auf **OK**. Die IP-Adresse wird zur Liste der vertrauenswürdigen IP-Adressen hinzugefügt.

So überprüfen Sie, ob die IP-Adresse hinzugefügt wurde:

1 Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie **Optionen** aus.

2 Klicken Sie auf das Symbol für **Vertrauenswürdige & gesperrte IP-Adressen**, und klicken Sie dann auf die Registerkarte **Vertrauenswürdige IP-Adressen**.

Die IP-Adresse wird aktiviert in der Liste der vertrauenswürdigen IP-Adressen angezeigt.

Sperren einer Adresse

Wenn eine IP-Adresse in Ihrem Protokoll eingehender Ereignisse angezeigt wird, bedeutet dies, dass Datenverkehr von dieser Adresse blockiert wurde. Folglich stellt das Sperren einer Adresse keinen zusätzlichen Schutz dar, es sei denn, der Computer verfügt über Anschlüsse, die über die Systemdienste-Funktion absichtlich geöffnet werden, bzw. der Computer weist eine Anwendung auf, die für den Empfang von Datenverkehr berechtigt ist.

Fügen Sie der Liste gesperrter IP-Adressen nur dann eine IP-Adresse hinzu, wenn Sie über einen oder mehrere Anschlüsse verfügen, die absichtlich geöffnet sind, und Sie Grund zu der Annahme haben, den Zugriff unterbinden zu müssen.

Wenn auf der Seite der eingehenden Ereignisse ein Ereignis angezeigt wird, das eine zu sperrende IP-Adresse enthält, können Sie Personal Firewall so konfigurieren, dass Verbindungen mit dieser Adresse in jedem Fall unterbunden werden.

Sie können die Seite der eingehenden Ereignisse, auf der die IP-Adressen des gesamten eingehenden Datenverkehrs aufgeführt werden, dazu verwenden, eine IP-Adresse zu sperren, die vermutlich die Quelle verdächtiger oder unerwünschter Internetaktivität bildet.

So fügen Sie eine IP-Adresse zur Liste der gesperrten IP-Adressen hinzu:

1 Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie anschließend **Eingehende Ereignisse** aus.

2 Die Seite der eingehenden Ereignisse listet die IP-Adressen des gesamten eingehenden Internetdatenverkehrs auf. Wählen Sie eine IP-Adresse aus, und wählen Sie eine der folgenden Vorgehensweisen:

- Klicken Sie mit der rechten Maustaste auf die IP-Adresse, und wählen Sie dann **Quell-IP-Adresse sperren** aus.
- Klicken Sie im Menü **Ich möchte** auf die Option **Diese Adresse sperren**.

3 Verwenden Sie im Dialogfeld „Regel für gesperrte IP-Adresse hinzufügen“ eine der folgenden Einstellungen zur Konfiguration einer Regel für gesperrte IP-Adressen:

- **Eine einzelne IP-Adresse**: Die zu sperrende IP-Adresse. Standardmäßig ist die IP-Adresse eingetragen, die Sie auf der Seite der eingehenden Ereignisse ausgewählt haben.
- **Ein IP-Adressbereich**: Die IP-Adressen zwischen der Adresse in „Von IP-Adresse“ und der Adresse in „An IP-Adresse“.
- **Ablaufdatum für diese Regel festlegen auf**: Datum und Uhrzeit, zu der die Regel für die gesperrte IP-Adresse abläuft. Wählen Sie die gewünschten Werte für Datum und Uhrzeit aus dem Dropdownmenü aus.
- **Beschreibung**: Bei Bedarf beschreiben Sie die neue Regel.
- Klicken Sie auf **OK**.

4 Klicken Sie im Dialogfeld auf **Ja**, um Ihre Einstellungen zu bestätigen. Klicken Sie auf **Nein**, um zum Dialogfeld „Regel für gesperrte IP-Adresse hinzufügen“ zurückzukehren.

Wenn Personal Firewall ein Ereignis von einer gesperrten Internetverbindung erkennt, wird eine Warnung entsprechend der angegebenen Methode auf der Seite „Warneinstellungen“ ausgegeben.

So überprüfen Sie, ob die IP-Adresse hinzugefügt wurde:

1 Klicken Sie auf die Registerkarte **Optionen**.

2 Klicken Sie auf das Symbol für **Vertrauenswürdige & gesperrte IP-Adressen**, und klicken Sie dann auf die Registerkarte **Gesperrte IP-Adressen**.

Die IP-Adresse wird aktiviert in der Liste der gesperrten IP-Adressen angezeigt.

Verwalten des Protokolls eingehender Ereignisse

Auf der Seite mit den eingehenden Ereignissen können Sie die Ereignisse im Protokoll eingehender Ereignisse verwalten, das erzeugt wird, wenn Personal Firewall unaufgeforderten Internetverkehr blockiert:

Archivieren des Protokolls eingehender Ereignisse

Sie können das aktuelle Protokoll der eingehenden Ereignisse archivieren, um sämtliche protokollierte eingehende Ereignisse einschließlich Datum und Uhrzeit, Quell-IP-Adressen, Hostnamen, Anschlüssen und Ereignisinformationen zu speichern. Sie sollten Ihr Protokoll eingehender Ereignisse regelmäßig archivieren, damit das Protokoll nicht zu groß wird.

So archivieren Sie das Protokoll eingehender Ereignisse:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie anschließend **Eingehende Ereignisse** aus.
2. Auf der Seite der eingehenden Ereignisse klicken Sie auf **Archiv**.
3. Klicken Sie im Dialogfeld „Protokoll archivieren“ auf **Ja**, um den Archivierungsvorgang fortzusetzen.
4. Klicken Sie auf **Speichern**, um das Archiv im Standardspeicherort zu speichern, oder navigieren Sie zu dem Speicherort, an dem das Archiv gespeichert werden soll.

Hinweis: Standardmäßig archiviert Personal Firewall automatisch das Protokoll eingehender Ereignisse. Aktivieren oder deaktivieren Sie die Option **Protokollierte Ereignisse automatisch archivieren** auf der Seite „Ereignisprotokolleinstellungen“, indem Sie das Häkchen setzen oder entfernen.

Anzeigen des archivierten Protokolls eingehender Ereignisse

Sie können zuvor archivierte Protokolle eingehender Ereignisse anzeigen. Das gespeicherte Archiv enthält Datum und Uhrzeit, Quell-IP-Adressen, Hostnamen, Anschlüsse und Ereignisinformationen zu den Ereignissen.

So zeigen Sie das archivierte Protokoll eingehender Ereignisse an:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie anschließend **Eingehende Ereignisse** aus.
2. Auf der Seite der eingehenden Ereignisse klicken Sie auf **Archive anzeigen**.
3. Suchen bzw. wählen Sie den Dateinamen des Archivs aus, und klicken Sie auf **Öffnen**.

Löschen des Inhalts des Protokolls eingehender Ereignisse

Sie können alle Informationen aus dem Protokoll eingehender Ereignisse löschen.

WARNUNG: Wenn Sie den Inhalt des Protokolls eingehender Ereignisse löschen, kann dieser nicht wiederhergestellt werden. Wenn Sie davon ausgehen, dass Sie das Ereignisprotokoll zukünftig noch benötigen, sollten Sie es stattdessen archivieren.

So löschen Sie das Protokoll eingehender Ereignisse:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und wählen Sie dann **Eingehende Ereignisse** aus.
2. Auf der Seite der eingehenden Ereignisse klicken Sie auf **Protokoll löschen**.
3. Klicken Sie im Dialogfeld auf **Ja**, um das Protokoll zu löschen.

Kopieren von Ereignissen in die Zwischenablage

Sie können ein Ereignis in die Zwischenablage kopieren, um es von dort aus in eine Textdatei im Windows-Editor einzufügen.

So kopieren Sie Ereignisse in die Zwischenablage:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und wählen Sie dann **Eingehende Ereignisse** aus.
2. Klicken Sie mit der rechten Maustaste auf das Ereignis im Protokoll eingehender Ereignisse.
3. Klicken Sie auf **Ausgewähltes Ereignis in Zwischenablage kopieren**.
4. Starten Sie Editor.
   - Geben Sie `notepad` in die Befehlszeile ein, oder klicken Sie auf die Windows-Schaltfläche **Start**, zeigen Sie auf **Programme**, dann auf **Zubehör**. Wählen Sie **Editor** aus.
5. Klicken Sie auf **Bearbeiten** und anschließend auf „Einfügen“. Der Ereignistext wird in Editor angezeigt. Wiederholen Sie diesen Schritt so oft, bis Sie alle erforderlichen Ereignisse in Editor eingefügt haben.
6. Speichern Sie die Editor-Datei an einem sicheren Ort.

Löschen von ausgewählten Ereignissen

Sie können Ereignisse aus dem Protokoll eingehender Ereignisse löschen.

So löschen Sie Ereignisse aus dem Protokoll eingehender Ereignisse:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie anschließend **Eingehende Ereignisse** aus.

2 Klicken Sie auf der Seite eingehender Ereignisse auf den zu löschenden Ereigniseintrag.

3 Klicken Sie im Menü „Bearbeiten“ auf **Ausgewähltes Ereignis löschen**. Das Ereignis wird aus dem Protokoll eingehender Ereignisse gelöscht.

Info zu Warnungen

Es wird Ihnen dringend empfohlen, sich mit den Warntypen vertraut zu machen, auf die Sie bei der Verwendung von Personal Firewall stoßen. Lesen Sie die folgenden Informationen über vorhandene Warntypen sowie mögliche Reaktionen, damit Sie sicher mit Warnungen umgehen können.

HINWEIS
Empfehlungen zu Warnungen unterstützen Sie bei der richtigen Handhabung einer Warnung. Wenn Warnungen mit zusätzlich angegebenen Empfehlungen angezeigt werden sollen, klicken Sie auf die Registerkarte **Optionen**, klicken Sie dann auf das Symbol **Warneinstellungen** , und wählen Sie dann in der Liste **Empfehlungen** entweder **Empfehlungen automatisch verwenden** (die Standardeinstellung) oder **Nur Empfehlungen anzeigen** aus.

Rote Warnungen

Rote Warnungen enthalten wichtige Informationen, die ein sofortiges Eingreifen erfordern:

- **Internetanwendung blockiert:** Diese Warnung wird angezeigt, wenn Personal Firewall eine Anwendung daran hindert, auf das Internet zuzugreifen. Wenn beispielsweise eine Warnung zu einem Trojaner angezeigt wird, verweigert McAfee diesem Programm automatisch den Internetzugriff und empfiehlt Ihnen, den Computer nach Viren zu durchsuchen.
- **Die Anwendung möchte auf das Internet zugreifen:** Diese Warnung wird angezeigt, wenn Personal Firewall Internet- oder Netzwerkverkehr bei neuen Anwendungen erkennt.
- **Die Anwendung wurde geändert:** Diese Warnung wird angezeigt, wenn Personal Firewall erkennt, dass eine Anwendung, der Sie zuvor Zugriff auf das Internet gewährt haben, geändert wurde. Falls Sie die Anwendung nicht vor kurzem aktualisiert haben, gehen Sie mit Bedacht vor, wenn Sie ihr Zugriff auf das Internet gewähren.
- **Anwendung fordert Serverzugriff an:** Diese Warnung wird angezeigt, wenn Personal Firewall erkennt, dass eine Anwendung, der Sie zuvor Zugriff auf das Internet gewährt haben, Internetzugriff als Server anfordert.

HINWEIS
Die Standardeinstellung für automatische Updates von Windows XP SP2 lädt Updates für das Windows-Betriebssystem und andere auf Ihrem Rechner ausgeführte Microsoft-Programme herunter und installiert diese, ohne dass Sie darüber benachrichtigt werden. Wenn eine Anwendung durch ein solches stilles Windows-Update geändert wurde, zeigt McAfee Personal Firewall bei der nächsten Ausführung der betreffenden Microsoft-Anwendung eine Meldung an.

WICHTIG
Anwendungen, die Internetzugriff für Online-Produktupdates benötigen (z. B. McAfee-Dienste), müssen Sie den Zugriff gewähren, um sie auf dem neuesten Stand zu halten.

Warnung „Internetanwendung blockiert“

Wenn eine Warnung zu einem Trojaner angezeigt wird (Abbildung 3-4), verweigert Personal Firewall diesem Programm automatisch den Internetzugriff und empfiehlt Ihnen, den Computer nach Viren zu durchsuchen. Wenn McAfee VirusScan nicht installiert ist, starten Sie McAfee SecurityCenter.

McAfee Personal Firewall Plus
Internetanwendung blockiert!
Die Anwendung code.exe wurde als bösartiges trojanisches Pferd erkannt. Der Zugang zum Internet wird ihr automatisch verweigert.
Pfad: C:\WINDOWS\Desktop\code.exe
McAfee empfiehlt...
Ihren Computer nach Viren zu durchsuchen.
Ich möchte...
Anwendungsprotokoll anzeigen
Starten Sie McAfee Security Center
Fortfahren

Abbildung 3-4. Warnung „Internetanwendung blockiert“

Zeigen Sie eine Kurzbeschreibung des Ereignisses an, und wählen Sie anschließend unter den folgenden Optionen aus:

- Klicken Sie auf **Weitere Informationen**, um über das Protokoll eingehender Ereignisse Details zu dem Ereignis anzuzeigen (weitere Informationen finden Sie unter *Info zur Seite Eingehende Ereignisse* auf Seite 65).
- Klicken Sie auf **McAfee VirusScan starten**, um den Computer nach Viren zu durchsuchen.

- Klicken Sie auf **Fortfahren**, wenn Sie keine zusätzlichen Maßnahmen ergreifen möchten.
- Klicken Sie auf **Abgehenden Zugriff gewähren**, um eine ausgehende Verbindung zuzulassen (**Eingeschränkte** Sicherheit).

Warnung „Die Anwendung möchte auf das Internet zugreifen“

Wenn Sie in den Optionen der Sicherheitseinstellungen die Einstellung **Standard** oder **Eingeschränkt** ausgewählt haben, gibt Personal Firewall eine Warnung (Abbildung 3-5) aus, wenn Internet- oder Netzwerkverbindungen für neue oder geänderte Anwendungen erkannt werden.

McAfee Personal Firewall Plus
Die Anwendung möchte auf das Internet zugreifen.
Das Programm Server fordert Zugriff auf das Internet an. Möchten Sie ihn gewähren?
Pfad: C:\WINDOWS\Desktop\server.exe \Server.exe
Ich möchte...
Zugriff gewähren
Zugriff einmal gewähren
Gesamten Zugriff blockieren
Hilfe bei der Auswahl

Abbildung 3-5. Warnung „Die Anwendung möchte auf das Internet zugreifen“

Wenn eine Warnung eingeblendet wird, die zur Vorsicht hinsichtlich der Gewährung von Internetzugriff für die Anwendung rät, können Sie auf **Klicken Sie hier, um weitere Informationen anzuzeigen** klicken, um weitere Informationen über die Anwendung zu erhalten. Diese Option wird nur dann in der Warnung angezeigt, wenn Personal Firewall für die Verwendung von Empfehlungen konfiguriert wurde.

McAfee erkennt das Programm, das auf das Internet zugreifen möchte, möglicherweise nicht (Abbildung 3-6).

McAfee Personal Firewall Plus
Die Anwendung fordert Serverzugriff an.
Die Anwendung Server fordert an, als Server fungieren und eingehende Verbindungen annehmen zu können. Möchten Sie ihr Serverzugriff gewähren?
Pfad: C:\WINDOWS\Desktop\server.exe \Server.exe
McAfee...
erkennt diese Anwendung nicht.
Informieren Sie McAfee über dieses Programm.
Ich möchte...
Zugriff einmal gewähren
Serverzugriff gewähren
Auf abgehenden Zugriff beschränken
Gesamten Zugriff blockieren
Hilfe bei der Auswahl

Abbildung 3-6. Warnung bei nicht erkannter Anwendung

Deshalb kann McAfee nicht empfehlen, wie Sie mit dem Programm verfahren sollen. Sie können die Anwendung auch an McAfee melden, indem Sie auf **Informieren Sie McAfee über dieses Programm** klicken. Es wird eine Webseite angezeigt, auf der Sie nach Informationen zu dem Programm gefragt werden. Übermitteln Sie so viele Informationen wie möglich.

Die übermittelten Informationen werden von unseren HackerWatch-Mitarbeitern in Verbindung mit anderen Tools verwendet, um festzustellen, ob ein Programm in unsere Datenbankliste der bekannten Programme aufgenommen werden soll, und wenn ja, wie Personal Firewall damit umgehen soll.

Zeigen Sie eine Kurzbeschreibung des Ereignisses an, und wählen Sie anschließend unter den folgenden Optionen aus:

- Klicken Sie auf **Zugriff gewähren**, um ausgehende und eingehende Internetverbindungen der Anwendung zuzulassen.
- Klicken Sie auf **Zugriff einmal gewähren**, um eine temporäre Internetverbindung der Anwendung zuzulassen. Der Anwendung wird der Zugriff nur solange gewährt, bis sie wieder geschlossen wird.
- Klicken Sie auf **Gesamten Zugriff blockieren**, um eine Internetverbindung zu verhindern.
- Klicken Sie auf Abgehenden Zugriff gewähren, um eine ausgehende Verbindung zuzulassen (**Eingeschränkte** Sicherheit).
- Klicken Sie auf **Hilfe bei der Auswahl**, um die Online-Hilfe zu Zugriffsberechtigungen von Anwendungen zu konsultieren.

Warnung „Die Anwendung wurde geändert“

Wenn Sie in den Optionen der Sicherheitseinstellungen die Einstellung **Vertrauenswürdig**, **Standard** oder **Eingeschränkt** ausgewählt haben, gibt Personal Firewall eine Warnung (Abbildung 3-7) aus, wenn eine Anwendung geändert wurde, der Sie zuvor den Internetzugriff gewährt haben. Falls Sie die fragliche Anwendung nicht erst vor kurzem aktualisiert haben, gehen Sie mit Bedacht vor, wenn Sie ihr Zugriff auf das Internet gewähren.

McAfee Personal Firewall Plus
Die Anwendung wurde geändert
Die Anwendung Windows Media Player wurde geändert, seit Sie sie zum ersten Mal auf das Internet zugreifen ließen. Soll sie weiterhin Zugriff auf das Internet erhalten?
Pfad: C:\Programme\Windows Media Player\WMPLAYER.EXE
Ich möchte...
Zugriff gewähren
Zugriff einmal gewähren
Gesamten Zugriff blockieren
Hilfe bei der Auswahl

Abbildung 3-7. Warnung „Die Anwendung wurde geändert“

Zeigen Sie eine Kurzbeschreibung des Ereignisses an, und wählen Sie anschließend unter den folgenden Optionen aus:

- Klicken Sie auf **Zugriff gewähren**, um ausgehende und eingehende Internetverbindungen der Anwendung zuzulassen.
- Klicken Sie auf **Zugriff einmal gewähren**, um eine temporäre Internetverbindung der Anwendung zuzulassen. Der Anwendung wird der Zugriff nur solange gewährt, bis sie wieder geschlossen wird.
- Klicken Sie auf **Gesamten Zugriff blockieren**, um eine Internetverbindung zu verhindern.
- Klicken Sie auf Abgehenden Zugriff gewähren, um eine ausgehende Verbindung zuzulassen (**Eingeschränkte** Sicherheit).
- Klicken Sie auf **Hilfe bei der Auswahl**, um die Online-Hilfe zu Zugriffsberechtigungen von Anwendungen zu konsultieren.

Warnung „Anwendung fordert Serverzugriff an“

Wenn Sie in den Optionen der Sicherheitseinstellungen die Einstellung **Eingeschränkt** ausgewählt haben, gibt Personal Firewall eine Warnung (Abbildung 3-8) aus, wenn eine Anwendung, der Sie zuvor den Zugriff auf das Internet gewährt haben, den Internetzugriff als Server angefordert hat.

McAfee Personal Firewall Plus
Die Anwendung fordert Serverzugriff an.
Die Anwendung Server fordert an, als Server fungieren und eingehende Verbindungen annehmen zu können. Möchten Sie ihr Serverzugriff gewähren?
Pfad: C:\WINDOWS\Desktop\server.exe \Server.exe
Ich möchte...
Zugriff einmal gewähren
Serverzugriff gewähren
Auf abgehenden Zugriff beschränken
Gesamten Zugriff blockieren
Hilfe bei der Auswahl

Abbildung 3-8. Warnung „Anwendung fordert Serverzugriff an“

Beispielsweise wird eine Warnung eingeblendet, wenn MSN Messenger Serverzugriff anfordert, um im Rahmen eines Chats eine Datei zu senden.

Zeigen Sie eine Kurzbeschreibung des Ereignisses an, und wählen Sie anschließend unter den folgenden Optionen aus:

- Klicken Sie auf **Zugriff einmal gewähren**, um einen temporären Internetzugriff der Anwendung zuzulassen. Der Anwendung wird der Zugriff nur solange gewährt, bis sie wieder geschlossen wird.
- Klicken Sie auf **Serverzugriff gewähren**, um ausgehende und eingehende Internetverbindungen der Anwendung zuzulassen.
- Klicken Sie auf **Auf abgehenden Zugriff beschränken**, um eingehende Internetverbindungen zu verhindern.
- Klicken Sie auf **Gesamten Zugriff blockieren**, um eine Internetverbindung zu verhindern.
- Klicken Sie auf **Hilfe bei der Auswahl**, um die Online-Hilfe zu Zugriffsberechtigungen von Anwendungen zu konsultieren. Grüne Warnungen

Grüne Warnungen

Grüne Warnungen benachrichtigen Sie bei Ereignissen in Personal Firewall, wenn beispielsweise einer Anwendung automatisch Internetzugriff gewährt wurde.

Programm darf auf das Internet zugreifen: Diese Warnung wird angezeigt, wenn Personal Firewall automatisch allen neuen Anwendungen Internetzugriff gewährt und Sie anschließend informiert (Sicherheitseinstellung **Vertrauenswürdig**). Ein Beispiel für eine geänderte Anwendung ist eine Anwendung mit geänderten Regeln, durch die der Anwendung automatisch der Internetzugriff erlaubt wird.

Warnung, dass Anwendung auf das Internet zugreifen darf

Wenn Sie in den Optionen für die Sicherheitseinstellungen die Einstellung **Vertrauenswürdig** ausgewählt haben, gewährt Personal Firewall automatisch allen neuen Anwendungen Internetzugriff und informiert Sie anschließend in Form einer Warnung (Abbildung 3-9).

McAfee Personal Firewall Plus
Programm darf auf das Internet zugreifen
Dem Programm MSN Messenger wurde automatisch Zugriff auf das Internet gewährt.
Pfad: C:\Programme\MSN Messenger \msnmsgr.exe
Anwendung erlaubt, weil...
McAfee diese Anwendung anerkennt.
Klicken Sie hier, um weitere Informationen anzuzeigen.
Ich möchte...
Anwendungsprotokoll anzeigen
Diesen Alarmtyp abschalten
Fortfahren

Abbildung 3-9. Programm darf auf das Internet zugreifen

Zeigen Sie eine Kurzbeschreibung des Ereignisses an, und wählen Sie anschließend unter den folgenden Optionen aus:

- Klicken Sie auf **Anwendungsprotokoll anzeigen**, um Details über das Internetanwendungsprotokoll zu dem Ereignis anzuzeigen (weitere Informationen finden Sie unter *Info zur Seite „Internetanwendungen“* auf Seite 63).
- Klicken Sie auf **Diesen Alarmtyp abschalten**, um die Anzeige dieses Warnungstyps zu unterdrücken.
- Klicken Sie auf **Fortfahren**, wenn Sie keine zusätzlichen Maßnahmen ergreifen möchten.
- Klicken Sie auf **Gesamten Zugriff blockieren**, um eine Internetverbindung zu verhindern.

Warnung „Die Anwendung wurde geändert“

Wenn Sie in den Optionen für die Sicherheitseinstellungen die Einstellung **Vertrauenswürdig** ausgewählt haben, gewährt Personal Firewall automatisch allen neuen und geänderten Anwendungen Internetzugriff. Zeigen Sie eine Kurzbeschreibung des Ereignisses an, und wählen Sie anschließend unter den folgenden Optionen aus:

- Klicken Sie auf **Anwendungsprotokoll anzeigen**, um Details über das Internetanwendungsprotokoll zu dem Ereignis anzuzeigen (weitere Informationen finden Sie unter *Info zur Seite „Internetanwendungen“* auf Seite 63).
- Klicken Sie auf **Diesen Alarmtyp abschalten**, um die Anzeige dieses Warnungstyps zu unterdrücken.
- Klicken Sie auf **Fortfahren**, wenn Sie keine zusätzlichen Maßnahmen ergreifen möchten.
- Klicken Sie auf **Gesamten Zugriff blockieren**, um eine Internetverbindung zu verhindern.

Blaue Warnungen

Blaue Warnungen enthalten Informationen; es ist jedoch keine Reaktion Ihrerseits erforderlich.

- **Versuch, eine Verbindung herzustellen, wurde blockiert:** Diese Warnung wird angezeigt, wenn Personal Firewall unerwünschten Internet- oder Netzwerkverkehr blockiert. („Vertrauenswürdig“, „Standard“ oder „Eingeschränkte Sicherheit“)

Warnung „Versuch, eine Verbindung herzustellen, wurde blockiert“

Wenn Sie die Sicherheitseinstellung **Vertrauenswürdig**, **Standard** oder **Eingeschränkt** ausgewählt haben, gibt Personal Firewall eine Warnung (Abbildung 3-10) aus, wenn unerwünschter Internet- oder Netzwerkverkehr blockiert wird.

McAfee Personal Firewall Plus
Versuch, eine Verbindung herzustellen, wurde blockiert
Ein Computer, mit dem Sie unter der IP-Adresse 192.168.1.40 kommuniziert haben, hat versucht, auf einen anderen als den erwarteten Anschluss (UDP Anschluss 1483) zuzugreifen.
Ich möchte...
Ereignisprotokoll anzeigen
Diese Adresse verfolgen
Diesen Alarmtyp abschalten
Fortfahren

Abbildung 3-10. Warnung „Versuch, eine Verbindung herzustellen, wurde blockiert“

Zeigen Sie eine Kurzbeschreibung des Ereignisses an, und wählen Sie anschließend unter den folgenden Optionen aus:

- Klicken Sie auf **Ereignisprotokoll anzeigen** , um über das Protokoll eingehender Ereignisse von Personal Firewall Details zu dem Ereignis anzuzeigen (weitere Informationen finden Sie unter *Info zur Seite Eingehende Ereignisse* auf Seite 65).
- Klicken Sie auf **Diese Adresse verfolgen**, um eine visuelle Verfolgung der IP-Adressen dieses Ereignisses durchzuführen.
- Klicken Sie auf **Diese Adresse sperren**, um zu verhindern, dass diese Adresse auf Ihren Computer zugreift. Die Adresse wird der Liste der gesperrten IP-Adressen hinzugefügt.
- Klicken Sie auf **Diese Adresse als vertrauenswürdig einstufen**, um dieser IP-Adresse den Zugriff auf Ihren Computer zu gewähren.
- Klicken Sie auf **Fortfahren**, wenn Sie keine zusätzlichen Maßnahmen ergreifen möchten.

McAfee Privacy Service 4

Willkommen bei McAfee Privacy Service

Die McAfee Privacy Service-Software bietet fortschrittlichen Schutz für Sie, Ihre Familie, Ihre persönlichen Daten und Ihren Computer.

Funktionen

Diese Version von McAfee Privacy Service enthält die folgenden Funktionen:

- Regeln für Internetzugriffszeiten – Verwenden Sie ein Zeitraster, um Tage und Zeiten festzulegen, zu denen ein Benutzer auf das Internet zugreifen darf.
- Benutzerdefinierte Stichwortfilterung – Filterung des Website-Zugriffs auf Basis von Stichwörtern, die der Administrator für bestimmte Altersstufen festlegt.
- Privacy Service-Sicherung und Wiederherstellung – Sie können Ihre Privacy Service-Einstellungen jederzeit speichern und wiederherstellen.
- Web Bug Blocker – Blockiert Web-Bugs (von möglicherweise gefährlichen Websites erhaltene Objekte), so dass diese nicht auf im Browser angezeigte Webseiten geladen werden.
- Pop-up Blocker – Verhindert die Anzeige von Popup-Fenstern, während Sie im Internet surfen.
- Shredder – McAfee Shredder schützt Ihre Privatsphäre durch das schnelle und sichere Vernichten unerwünschter Dateien.

Der Administrator

Der Administrator gibt an, welche Benutzer auf das Internet zugreifen dürfen, wann sie das Internet verwenden dürfen und zu welchem Zweck.

HINWEIS
Der Administrator wird als Erwachsener angesehen und darf demzufolge auf alle Websites zugreifen. Er wird jedoch aufgefordert, die Übermittlung von hinzugefügten persönlichen Daten zu ermöglichen bzw. zu vermeiden.

Setup-Assistent

Der Setup-Assistent dient zur Erstellung des Administrators (sofern dies nicht bereits geschehen ist), zur Verwaltung globaler Einstellungen, zur Eingabe persönlicher Informationen und zum Hinzufügen von Benutzern.

HINWEIS

Merken Sie sich Ihr Administratorkennwort und Ihre Antwort auf die Sicherheitsfrage, damit Sie sich bei Privacy Service anmelden können. Wenn Sie sich nicht anmelden können, können Sie Privacy Service und das Internet nicht verwenden. Halten Sie Ihr Kennwort geheim, so dass nur Sie die Privacy Service-Einstellungen ändern können.

Für manche Websites müssen Cookies aktiviert sein, damit die Websites ordnungsgemäß funktionieren.

Privacy Service akzeptiert stets Cookies von McAfee.com.

Wiederbeschaffen des Administratorkennworts

Wenn Sie das Administratorkennwort vergessen, können Sie Ihr Kennwort mithilfe der Sicherheitsinformationen, die Sie bei der Erstellung des Administratorprofils eingegeben haben, aufrufen.

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Systemablage, zeigen Sie auf **McAfee Privacy Service** und wählen Sie anschließend **Anmelden**.
2. Wählen Sie **Administrator** im Pulldown-Menü **Benutzername**.
3. Klicken Sie auf **Kennwort vergessen?**.
4. Geben Sie die Antwort auf die angezeigte Sicherheitsfrage ein, und klicken Sie anschließend auf **Kennwort abrufen**. Eine Meldung, die Ihr Kennwort enthält, wird angezeigt. Sollten Sie die Antwort auf die Sicherheitsfrage vergessen, müssen Sie McAfee Privacy Service im abgesicherten Modus deinstallieren (nur Windows 2000 und Windows XP).

Der Startbenutzer

Der Startbenutzer wird automatisch bei Privacy Service angemeldet, wenn der Computer gestartet wird.

Wenn beispielsweise ein bestimmter Benutzer den Computer oder das Internet häufiger verwendet als andere Benutzer, können Sie den entsprechenden Benutzer als Startbenutzer definieren. Wenn der Startbenutzer den Computer verwendet, muss er sich nicht bei Privacy Service anmelden.

Wenn Sie kleine Kinder haben, können Sie als Startbenutzer auch das jüngste Kind festlegen. Auf diese Weise kann sich ein älterer Benutzer, wenn er den Computer verwendet, vom Konto des jüngeren Benutzers abmelden und sich anschließend wieder mit seinem eigenen Benutzernamen und Kennwort anmelden. So werden jüngere Benutzer vor ungeeigneten Websites geschützt.

Öffnen von McAfee Privacy Service

Wenn Sie McAfee Privacy Service installieren, wird das McAfee-Symbol in der Windows-Taskleiste in der Nähe der Systemuhr eingeblendet. Über das McAfee-Symbol können Sie auf McAfee Privacy Service, McAfee Security Center und andere McAfee-Produkte, die auf Ihrem Computer installiert sind, zugreifen.

Öffnen von und Anmelden bei Privacy Service

So öffnen Sie Privacy Service:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **McAfee Privacy Service**, und klicken Sie dann auf **Anmelden**.
2. Wählen Sie Ihren Benutzernamen im Pulldown-Menü **Benutzername**.
3. Geben Sie in das Feld **Kennwort** Ihr Kennwort ein.
4. Klicken Sie auf **Anmelden**.

Deaktivieren von Privacy Service

Sie müssen bei Privacy Service als Administrator angemeldet sein, um Privacy Service zu deaktivieren.

So deaktivieren Sie Privacy Service:

Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **McAfee Privacy Service**, und klicken Sie dann auf **Abmelden**.

HINWEIS
Falls an Stelle von **Abmelden** die Option **Anmelden** vorhanden ist, sind Sie bereits abgemeldet.

Aktualisieren von McAfee Privacy Service

McAfee SecurityCenter sucht regelmäßig nach Updates für Privacy Service, wenn Ihr Computer eingeschaltet und mit dem Internet verbunden ist. Wenn eine Aktualisierung verfügbar ist, werden Sie von McAfee SecurityCenter aufgefordert, Privacy Service zu aktualisieren.

Um manuell nach Updates zu suchen, klicken Sie auf die Schaltfläche Updates im oberen Bereich.

Benutzer hinzufügen

Um Benutzer hinzuzufügen, müssen Sie sich bei Privacy Service als Administrator anmelden.

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste.
2. Zeigen Sie auf **McAfee Privacy Service** und wählen Sie **Benutzer verwalten**. Das Dialogfeld **Benutzer auswählen** wird geöffnet.
3. Klicken Sie auf **Hinzufügen**, und geben Sie den Namen des neuen Benutzers in das Feld **Benutzername** ein.

Festlegen des Kennworts

1. Geben Sie in das Feld **Kennwort** ein Kennwort ein. Das Kennwort darf bis zu 50 Zeichen umfassen und groß geschriebene sowie klein geschriebene Buchstaben sowie Zahlen enthalten.
2. Geben Sie das Kennwort erneut in das Feld **Kennwort bestätigen** ein.
3. Wählen Sie **Dieser Benutzer ist der Startbenutzer**, wenn Sie diesen Benutzer als Startbenutzer festlegen möchten.
4. Klicken Sie auf **Weiter**.

Berücksichtigen Sie bei der Zuweisung des Kennworts das Alter der betreffenden Person. Wenn Sie beispielsweise einem Kind ein Kennwort zuweisen, sollte das Kennwort einfach sein. Wenn Sie einem älteren Teenager oder einem Erwachsenen ein Kennwort zuweisen, sollten Sie ein komplexeres Kennwort verwenden.

Festlegen der Altersgruppe

Wählen Sie die entsprechende altersabhängige Einstellung, und klicken Sie anschließend auf **Weiter**.

Festlegen des Cookie Blocker

Wählen Sie die geeignete Option aus, und klicken Sie anschließend auf **Weiter**.

- **Alle Cookies ablehnen** – Verhindert, dass Websites an Ihren Computer gesendete Cookies lesen können. Einige Websites funktionieren nur ordnungsgemäß, wenn Sie Cookies aktivieren.
- **Cookies müssen vom Benutzer manuell akzeptiert werden** – Sie können von Fall zu Fall entscheiden, ob Cookies akzeptiert oder abgelehnt werden sollen. Privacy Service benachrichtigt Sie, wenn eine Website, die Sie anzeigen möchten, ein Cookie an Ihren Computer senden möchte. Nachdem Sie Ihre Entscheidung getroffen haben, werden Sie zu diesem Cookie nicht mehr befragt.
- **Alle Cookies akzeptieren** – Lässt zu, dass Websites die an Ihren Computer gesendeten Cookies lesen können.

HINWEIS
Manche Websites funktionieren nur ordnungsgemäß, wenn Cookies aktiviert sind.

Privacy Service akzeptiert Cookies von McAfee immer.

Festlegen der Internetzugriffszeiten

So gewähren Sie uneingeschränkten Internetzugriff:

1. Wählen Sie **Internetzugriff immer möglich**.
2. Klicken Sie auf **Erstellen**. Der neue Benutzer wird in der Liste „Benutzer auswählen“ angezeigt.

So gewähren Sie eingeschränkten Internetzugriff:

1. Wählen Sie **Internetzugriff einschränken**, und klicken Sie anschließend auf **Bearbeiten**.
2. Ziehen Sie den Mauszeiger auf der Seite „Zugriffszeiten für das Internet“ über das Zeitraster, um die Zeit und den Tag für den Zugriff des Benutzers auf das Internet auszuwählen.
   Sie können die Zeitbegrenzungen in Dreißig-Minuten-Intervallen festlegen. Grüne Bereiche des Rasters stehen für Zeiträume, in denen ein Benutzer auf das Internet zugreifen kann. Rote Bereiche zeigen an, wann der Benutzer nicht auf das Internet zugreifen kann. Sollte ein Benutzer versuchen, das Internet zu einem Zeitpunkt zu verwenden, zu dem ihm dies nicht gestattet ist, zeigt Privacy Service eine Meldung mit dem Hinweis an, dass der Benutzer das Internet zum aktuellen Zeitpunkt nicht verwenden darf. Um die Zeiträume zu ändern, in denen ein Benutzer auf das Internet zugreifen darf, ziehen Sie den Mauszeiger über die grünen Bereiche des Rasters.
3. Klicken Sie auf **Fertig**.

4 Klicken Sie auf **Erstellen**. Der neue Benutzer wird auf der Seite „Benutzer auswählen“ angezeigt. Sollte ein Benutzer versuchen, das Internet zu einem Zeitpunkt zu verwenden, zu dem ihm dies nicht gestattet ist, zeigt Privacy Service eine Meldung mit dem Hinweis an, dass der Benutzer das Internet zum aktuellen Zeitpunkt nicht verwenden darf.

So verhindern Sie Internetzugriff:

- Wählen Sie **Internetzugriff einschränken**, und klicken Sie anschließend auf **Erstellen**. Wenn der Benutzer den Computer verwendet, wird er aufgefordert, sich bei Privacy Service anzumelden. Der Benutzer darf den Computer, nicht jedoch das Internet verwenden.

Bearbeiten von Benutzern

Um Benutzer zu bearbeiten, müssen Sie sich bei Privacy Service als Administrator anmelden.

Ändern von Kennwörtern

1 Wählen Sie den Benutzer aus, dessen Informationen Sie ändern möchten, und klicken Sie auf **Bearbeiten**.

2 Wählen Sie **Kennwort** aus, und geben Sie das neue Kennwort des Benutzers in das Feld **Neues Kennwort** ein. Das Kennwort darf bis zu 50 Zeichen umfassen und groß bzw. klein geschriebene Buchstaben sowie Zahlen enthalten.

3 Geben Sie dasselbe Kennwort in das Feld **Kennwort bestätigen** ein, und klicken Sie anschließend auf **Übernehmen**.

4 Klicken Sie im Bestätigungsdialogfeld auf **OK**.

HINWEIS
Ein Administrator kann das Kennwort eines Benutzers ändern, ohne dessen aktuelles Kennwort zu kennen.

Ändern der Informationen eines Benutzers

1 Wählen Sie den Benutzer aus, dessen Informationen Sie ändern möchten, und klicken Sie auf **Bearbeiten**.

2 Wählen Sie **Benutzerinformationen** aus.

3 Geben Sie den neuen Benutzernamen in das Feld **Neuer Benutzername** ein.

4 Klicken Sie auf **Übernehmen** und anschließend im Bestätigungsdialogfeld auf **OK**.

5 Wenn Sie einen Benutzer dahin gehend einschränken möchten, dass dieser nur die Websites in der Liste Zulässige Websites anzeigen darf, wählen Sie die Option **Diesen Benutzer auf Websites einschränken in „Zulässige Websites“**.

Ändern der Cookie Blocker-Einstellung

1 Wählen Sie den Benutzer aus, dessen Informationen Sie ändern möchten, und klicken Sie auf **Bearbeiten**.

2 Wählen Sie **Cookies**, und klicken Sie auf die geeignete Option.

- **Alle Cookies ablehnen** – Verhindert, dass Websites an Ihren Computer gesendete Cookies lesen können. Einige Websites funktionieren nur ordnungsgemäß, wenn Sie Cookies aktivieren.
- **Cookies müssen vom Benutzer manuell akzeptiert werden** – Sie können von Fall zu Fall entscheiden, ob Cookies akzeptiert oder abgelehnt werden sollen. Privacy Service benachrichtigt Sie, wenn eine Website, die Sie anzeigen möchten, ein Cookie an Ihren Computer senden möchte. Nachdem Sie Ihre Entscheidung getroffen haben, werden Sie zu diesem Cookie nicht mehr befragt.
- **Alle Cookies akzeptieren** – Lässt zu, dass Websites die an Ihren Computer gesendeten Cookies lesen können.

3 Klicken Sie auf **Übernehmen** und anschließend im Bestätigungsdialogfeld auf **OK**.

Bearbeiten der Liste für akzeptierte und abgelehnte Cookies

1 Wählen Sie **Cookies müssen vom Benutzer manuell akzeptiert werden**, und klicken Sie auf **Bearbeiten**, um anzugeben, von welchen Websites Cookies gelesen werden dürfen.

2 Geben Sie die zu ändernde Liste an, indem Sie die Option **Websites, die Cookies anlegen dürfen** oder **Websites, die keine Cookies anlegen dürfen** auswählen.

3 Geben Sie im Feld **http://** die Adresse der Website ein, von der Sie Cookies entweder annehmen oder ablehnen.

4 Klicken Sie auf **Hinzufügen**. Die Website wird in der Liste „Website“ angezeigt.

5 Klicken Sie auf **Fertig**, nachdem Sie die Änderungen durchgeführt haben.

HINWEIS
Manche Websites funktionieren nur ordnungsgemäß, wenn Cookies aktiviert sind.

Privacy Service akzeptiert Cookies von McAfee immer.

Ändern der Altersgruppe

1. Wählen Sie den Benutzer aus, dessen Informationen Sie ändern möchten, und klicken Sie auf **Bearbeiten**.
2. Wählen Sie **Altersgruppe**.
3. Wählen Sie eine neue Altersgruppe für den Benutzer aus, und klicken Sie auf **Übernehmen**.
4. Klicken Sie im Bestätigungsdialogfeld auf **OK**.

Ändern der Internetzugriffszeiten

1. Wählen Sie den Benutzer aus, dessen Informationen Sie ändern möchten, und klicken Sie auf **Bearbeiten**.
2. Klicken Sie auf **Zugriffszeiten**, und gehen Sie wie folgt vor:

So gewähren Sie dem Benutzer einen ständigen Internetzugriff:

1. Wählen Sie **Internetzugriff immer möglich**, und klicken Sie auf **Übernehmen**.
2. Klicken Sie im Bestätigungsdialogfeld auf **OK**.

So schränken Sie den Internetzugriff für den Benutzer ein:

1. Wählen Sie **Internetzugriff einschränken**, und klicken Sie auf **Bearbeiten**.
2. Wählen Sie auf der Seite „Zugriffszeiten für das Internet“ ein grünes oder rotes Quadrat aus, und ziehen Sie den Mauszeiger über das Raster, um bestehende Zeiten und Tage für den Zugriff des Benutzers auf das Internet zu ändern. Sie können die Zeitbegrenzungen in Dreißig-Minuten-Intervallen festlegen. Grüne Bereiche des Rasters stehen für Zeiträume, in denen ein Benutzer auf das Internet zugreifen kann. Rote Bereiche zeigen an, wann der Benutzer nicht auf das Internet zugreifen kann. Sollte ein Benutzer versuchen, das Internet zu einem Zeitpunkt zu verwenden, zu dem ihm dies nicht gestattet ist, zeigt Privacy Service eine Meldung mit dem Hinweis an, dass der Benutzer das Internet zum aktuellen Zeitpunkt nicht verwenden darf.
3. Klicken Sie auf **Übernehmen**.
4. Klicken Sie auf der Seite Zugriffszeiten auf **OK**.
5. Klicken Sie im Dialogfeld McAfee Privacy Service auf **OK**.

Ändern des Startbenutzers

1. Wählen Sie den Benutzer aus, den Sie als Startbenutzer festlegen möchten, und klicken Sie auf **Bearbeiten**.
2. Wählen Sie **Benutzerinformationen** aus.
3. Wählen Sie **Dieser Benutzer ist der Startbenutzer**.
4. Klicken Sie auf **Übernehmen** und anschließend im Bestätigungsdialogfeld auf **OK**.

> **HINWEIS**
> Falls bereits ein Startbenutzer vorhanden ist, müssen Sie dessen Auswahl als Startbenutzer nicht aufheben.

Entfernen von Benutzern

1. Wählen Sie den zu entfernenden Benutzer aus, und klicken Sie dann auf **Entfernen**.
2. Klicken Sie im Bestätigungsdialogfeld auf **Ja**.
3. Schließen Sie das Privacy Service-Fenster, nachdem Sie die Änderungen durchgeführt haben.

Optionen

Sie müssen sich bei Privacy Service als Administrator anmelden, um Privacy Service-Optionen zu konfigurieren.

Blockieren von Websites

1. Klicken Sie auf **Optionen**, und wählen Sie anschließend **Liste der blockierten Websites**.
2. Geben Sie in das Feld **http://** den URL der Website ein, die Sie blockieren möchten, und klicken Sie anschließend auf **Hinzufügen**. Die Website wird in der Liste **Blockierte Websites** angezeigt.

> **HINWEIS**
> Benutzer (einschließlich Administratoren), die zur Gruppenebene „Erwachsener“ gehören, können auf alle Websites zugreifen, auch wenn die gewünschten Websites in der Liste „Blockierte Websites“ enthalten sind. Zum Testen von blockierten Websites müssen Administratoren sich als minderjährige Benutzer anmelden.

Zulassen von Websites

Der Administrator kann allen Benutzern den Zugriff auf bestimmte Websites gestatten. Hierdurch werden die Standardeinstellungen von Privacy Service und zur Liste blockierter Websites hinzugefügte Sites außer Kraft gesetzt.

1. Klicken Sie auf **Optionen**, und wählen Sie anschließend **Liste der zulässigen Websites**.
2. Geben Sie in das Feld **http://** den URL der Website ein, die Sie zulassen möchten, und klicken Sie anschließend auf **Hinzufügen**. Die Website wird in der Liste **Zulässige Websites** angezeigt.

Blockieren von Informationen

Der Administrator kann verhindern, dass andere Benutzer bestimmte persönliche Informationen über das Internet versenden (der Administrator kann diese Art von Informationen dennoch senden).

Wenn Privacy Service erkennt, dass persönliche Daten gesendet werden sollen, geschieht Folgendes:

- Falls Sie der Administrator sind, werden Sie aufgefordert zu entscheiden, ob die Informationen gesendet werden.
- Wenn der angemeldete Benutzer nicht der Administrator ist, wird die blockierte Information durch *MFEMFEMFE* ersetzt. Wenn Sie beispielsweise die E-Mail *Lance Armstrong gewinnt Tour* senden und Armstrong als persönliche Information festgelegt wurde, die blockiert werden soll, so wird die E-Mail tatsächlich als *Lance MFEMFEMFE gewinnt Tour* versendet.

Hinzufügen von Informationen

1. Klicken Sie auf **Optionen**, und wählen Sie anschließend **Informationen blockieren**.
2. Klicken Sie auf **Hinzufügen**. Das Pulldown-Menü **Typ auswählen** wird angezeigt.
3. Wählen Sie den Informationstyp, der blockiert werden soll.
4. Geben Sie die Informationen in die entsprechenden Felder ein, und klicken Sie auf **OK**. Die von Ihnen eingegebenen Informationen werden in der Liste angezeigt.

Bearbeiten von Informationen

1. Klicken Sie auf **Optionen**, und wählen Sie anschließend **Informationen blockieren**.
2. Wählen Sie die Informationen aus, die Sie ändern möchten, und klicken Sie auf **Bearbeiten**.
3. Nehmen Sie die gewünschten Änderungen vor, und klicken Sie anschließend auf **OK**. Sollten die Informationen nicht geändert werden müssen, klicken Sie auf **Abbrechen**.

Entfernen persönlicher Daten

1. Klicken Sie auf **Optionen**, und wählen Sie anschließend **Informationen blockieren**.
2. Wählen Sie die Informationen aus, die Sie ändern möchten, und klicken Sie auf **Entfernen**.
3. Klicken Sie im Bestätigungsdialogfeld auf **Ja**.

Blockieren von Web-Bugs

Web-Bugs sind kleine Grafikdateien, die Nachrichten an Dritte senden können und auf diese Weise beispielsweise Ihre Internet-Gewohnheiten verfolgen oder persönliche Daten an eine externe Datenbank übertragen können. Dritte können dann mithilfe dieser Informationen Benutzerprofile erstellen.

Um zu verhindern, dass Web-Bugs auf im Browser angezeigten Seiten geladen werden, wählen Sie die Option **Web-Bugs auf diesem Computer blockieren** aus.

Blockieren von Werbung

Werbungen sind normalerweise Grafiken, die von Drittanbieterdomänen auf einer Webseite oder in einem Popup-Fenster bereitgestellt werden. Privacy Service blockiert keine Werbeanzeigen, die von derselben Domäne wie der Host-Webseite bereitgestellt werden.

Popup-Fenster sind eingeblendete Browser-Fenster, die unerwünschte Werbungen präsentieren und automatisch angezeigt werden, wenn Sie eine Website besuchen. Privacy Service blockiert nur die Popup-Fenster, die beim Laden einer Webseite automatisch geladen werden. Popup-Fenster, die durch Klicken auf einen Link aufgerufen werden, werden von Privacy Service nicht blockiert. Wenn Sie ein blockiertes Popup-Fenster anzeigen möchten, halten Sie die STRG-Taste gedrückt, und aktualisieren Sie die Webseite.

Konfigurieren Sie Privacy Service so, dass Werbeanzeigen und Popup-Fenster bei Verwendung des Internets blockiert werden.

1. Klicken Sie auf **Optionen**, und wählen Sie anschließend **Werbung blockieren**.
2. Wählen Sie die entsprechende Option aus.
   - **Werbung auf diesem Computer blockieren** – Blockiert Werbeanzeigen, während Sie das Internet verwenden.
   - **Popups auf diesem Computer blockieren** – Blockiert Popup-Fenster, während Sie das Internet verwenden.
3. Klicken Sie auf **Übernehmen** und anschließend im Bestätigungsdialogfeld auf **OK**.

Wenn Sie das Blockieren von Popup-Fenstern deaktivieren möchten, klicken Sie mit der rechten Maustaste auf die Webseite, zeigen Sie auf **McAfee Pop-Up Blocker**, und deaktivieren Sie die Option **Pop-up Blocker aktivieren**.

Zulassen von Cookies von bestimmten Websites

Wenn Sie Cookies blockieren oder festlegen, dass Sie durch eine Meldung gefragt werden müssen, bevor Sie die Cookies akzeptieren, und feststellen, dass bestimmte Websites nicht ordnungsgemäß funktionieren, sollten Sie Privacy Service so konfigurieren, dass die Site die Cookies lesen darf.

1. Klicken Sie auf **Optionen**, und wählen Sie anschließend **Cookies**.
2. Geben Sie in das Feld **http://** die Adresse der Website ein, die ihre Cookies lesen können muss, und klicken Sie anschließend auf **Hinzufügen**. Die Adresse wird in der Liste **Cookie-Websites akzeptieren** angezeigt.

Ereignisprotokoll

Um das Ereignisprotokoll anzuzeigen, müssen Sie sich bei Privacy Service als Administrator anmelden. Wählen Sie im Anschluss daran die Option **Ereignisprotokoll**, und klicken Sie auf einen beliebigen Protokolleintrag, um die zugehörigen Details anzuzeigen. Um zu speichern oder ein gespeichertes Protokoll anzuzeigen, wählen Sie die Registerkarte Gespeicherte Protokolle.

Datum und Uhrzeit

Standardmäßig zeigt das Ereignisprotokoll die Informationen in chronologischer Reihenfolge an, wobei die neuesten Ereignisse am Anfang angezeigt werden. Sollten die Einträge des Ereignisprotokolls nicht in chronologischer Reihenfolge angezeigt werden, klicken Sie auf die Kopfzeile Datum und Uhrzeit.

Das Datum wird im Format Monat/Tag/Jahr, die Uhrzeit im Format A.M./P.M. angezeigt.

Benutzer

Der Benutzer ist die Person, die zum Zeitpunkt der Ereigniserfassung durch Privacy Service angemeldet war und auf das Internet zugegriffen hat.

Zusammenfassung

Zusammenfassungen bieten eine kurze, präzise Beschreibung darüber, was Privacy Service zum Schutz der Benutzer vornimmt und welche Vorgänge die Benutzer im Internet durchführen.

Ereignisdetails

Im Feld Ereignisdetails werden Eintragsdetails angezeigt.

Speichern des aktuellen Protokolls

Die Seite „Aktuelles Protokoll“ zeigt Informationen über kürzlich erfolgte Verwaltungs- und Benutzeraktionen an. Sie können diese Informationen speichern, um sie zu einem späteren Zeitpunkt aufzurufen.

So speichern Sie ein aktuelles Protokoll:

1. Melden Sie sich bei Privacy Service als Administrator an.
2. Wählen Sie **Ereignisprotokoll**.
3. Auf der Seite „Aktuelles Protokoll“ klicken Sie auf **Protokoll speichern**.
4. Geben Sie in das Feld **Dateiname** den Namen für die Protokolldatei ein.
5. Klicken Sie auf **Speichern**.

Anzeigen von gespeicherten Protokollen

Die Seite „Aktuelles Protokoll“ zeigt Informationen über kürzlich erfolgte Verwaltungs- und Benutzeraktionen an. Sie können diese Informationen speichern, um sie zu einem späteren Zeitpunkt aufzurufen.

So zeigen Sie ein gespeichertes Protokoll an:

1. Melden Sie sich bei Privacy Service als Administrator an.
2. Wählen Sie **Ereignisprotokoll**.
3. Auf der Seite „Aktuelles Protokoll“ klicken Sie auf **Protokoll öffnen**.
4. Wählen Sie im Dialogfeld **Wählen Sie ein gespeichertes Protokoll aus, das angezeigt werden soll** die Sicherungsdatei für die Datenbank aus, und klicken Sie anschließend auf **Öffnen**.

Dienstprogramme

Um auf die Dienstprogramme zuzugreifen, müssen Sie sich bei Privacy Service als Administrator anmelden. Klicken Sie anschließend auf **Dienstprogramme**.

Um Dateien, Ordner oder den gesamten Inhalt von Laufwerken zu entfernen, klicken Sie auf **McAfee Shredder**. Zum Speichern Ihrer Privacy Service-Datenbankeinstellungen klicken Sie auf **Sicherung**. Um Ihre Einstellungen wiederherzustellen, klicken Sie auf **Wiederherstellen**.

Dauerhaftes Löschen von Dateien mithilfe von McAfee Shredder

McAfee Shredder schützt Ihre Privatsphäre durch das schnelle und sichere Vernichten unerwünschter Dateien.

Gelöschte Dateien können von Ihrem Computer auch dann wiederhergestellt werden, nachdem Sie den Papierkorb geleert haben. Wenn Sie eine Datei löschen, kennzeichnet Windows den frei gewordenen Platz auf der Festplatte zwar als nicht mehr verwendet, die Datei ist jedoch noch vorhanden.

Warum Windows Dateireste zurücklässt

Um eine Datei dauerhaft zu löschen, müssen Sie die vorhandene Datei wiederholt mit neuen Daten überschreiben. Würde Microsoft Windows Dateien sicher löschen, wären sämtliche Dateivorgänge sehr langsam. Durch das Vernichten eines Dokuments wird nicht immer verhindert, dass das Dokument wiederhergestellt wird, da einige Programme temporäre verborgene Kopien geöffneter Dokumente erstellen. Falls Sie Dokumente, die Sie in Explorer anzeigen, lediglich vernichten, sind möglicherweise nach wie vor temporäre Kopien jener Dokumente vorhanden. Es empfiehlt sich, in regelmäßigen Abständen den freien Speicherplatz auf der Festplatte zu vernichten, um sicherzustellen, dass diese temporären Kopien dauerhaft gelöscht werden.

HINWEIS
Mit forensischen Computer-Tools können Steuererklärungen, Lebensläufe oder andere Dokumente, die von Ihnen gelöscht wurden, wiederbeschafft werden.

Was McAfee Shredder löscht

Mit McAfee Shredder können Sie Folgendes sicher und dauerhaft löschen:

- Eine(n) oder mehrere Dateien oder Ordner
- Einen gesamten Datenträger
- Beim Surfen im Internet hinterlassene Spuren

Dauerhaftes Löschen von Dateien in Windows-Explorer

So vernichten Sie eine Datei über Windows-Explorer:

1. Öffnen Sie Windows-Explorer, und wählen Sie die Datei oder die Dateien aus, die Sie vernichten möchten.
2. Klicken Sie mit der rechten Maustaste auf Ihre Auswahl, zeigen Sie auf **Senden an**, und wählen Sie anschließend **McAfee Shredder** aus.

Leeren des Papierkorbs unter Windows

Wenn sich in Ihrem Papierkorb Dateien befinden, bietet McAfee Shredder eine sehr sichere Methode zum Löschen des Papierkorbs.

So vernichten Sie den Inhalt des Papierkorbs:

1. Klicken Sie auf dem Windows-Desktop mit der rechten Maustaste auf Papierkorb.
2. Wählen Sie **Papierkorb vernichten**, und befolgen Sie die Anweisungen auf dem Bildschirm.

Anpassen der Shredder-Einstellungen

Sie haben folgende Möglichkeiten:

- Festlegen der Anzahl der Vernichtungsschritte.
- Anzeigen einer Warnmeldung beim Vernichten von Dateien.
- Überprüfen der Festplatte auf Fehler vor dem Vernichtungsvorgang.
- Hinzufügen von McAfee Shredder zum Menü Senden an
- Anlegen eines Shredder-Symbols auf dem Windows-Desktop.

Wenn Sie die Shredder-Einstellungen anpassen möchten, öffnen Sie McAfee Shredder, klicken Sie auf **Eigenschaften**, und befolgen Sie die Anweisungen auf dem Bildschirm.

Sichern der Privacy Service-Datenbank

Sie haben zwei Möglichkeiten, um die Privacy Service-Datenbank wiederherzustellen. Wird Ihre Datenbank beschädigt oder gelöscht, werden Sie von Privacy Service aufgefordert, die Privacy Service-Datenbank wiederherzustellen. Sie können Ihre Datenbankeinstellungen auch wiederherstellen, während Privacy Service ausgeführt wird.

1. Klicken Sie auf **Dienstprogramme**, und wählen Sie anschließend **Sicherung**.
2. Klicken Sie auf **Durchsuchen**, um einen Speicherort für die Datenbankdatei auszuwählen, und klicken Sie dann auf **OK**.
3. Geben Sie in das Feld **Kennwort** ein Kennwort ein.
4. Geben Sie das Kennwort erneut in das Feld **Kennwort bestätigen** ein, und klicken Sie auf **Sicherung**.
5. Klicken Sie im Bestätigungsdialogfeld auf **OK**.
6. Schließen Sie das Privacy Service-Fenster, nachdem der Vorgang abgeschlossen ist.

HINWEIS
Halten Sie dieses Kennwort geheim, und vergessen Sie es nicht. Sie können die Privacy Service-Einstellungen ohne dieses Kennwort nicht wiederherstellen.

Wiederherstellen der Sicherungsdatenbank

1. Privacy Service bietet zwei Möglichkeiten zum Wiederherstellen Ihrer ursprünglichen Einstellungen:
   - Laden Sie Ihre Sicherungsdatenbank, wenn Privacy Service Sie auffordert, Ihre Einstellungen wiederherzustellen, weil die Datenbank beschädigt oder gelöscht wurde.
   - Laden Sie Ihre Sicherungsdatenbank, während Privacy Service ausgeführt wird.

So stellen Sie Ihre Privacy Service-Einstellungen wieder her, wenn Sie dazu aufgefordert werden:

1. Klicken Sie auf **Durchsuchen**, um den Speicherort der Datei anzugeben.
2. Geben Sie in das Feld **Kennwort** Ihr Kennwort ein.
3. Klicken Sie auf **Wiederherstellen**.
   Falls Sie die Privacy Service-Datenbank nicht gesichert oder Ihr Sicherungskennwort vergessen haben, oder falls die Wiederherstellung der Datenbank nicht funktioniert, nehmen Sie bitte eine Deinstallation und erneute Installation von Privacy Service vor.

So stellen Sie Ihre Privacy Service-Einstellungen wieder her, während Privacy Service ausgeführt wird:

1. Klicken Sie auf die Registerkarte **Dienstprogramme**.
2. Klicken Sie auf **Wiederherstellen**.

3. Klicken Sie auf **Durchsuchen**, und geben Sie den Pfad und den Namen der Sicherungsdatei ein.
4. Klicken Sie auf **Öffnen**.
5. Geben Sie in das Feld **Kennwort** Ihr Kennwort ein.
6. Klicken Sie auf **Wiederherstellen**, und klicken sie anschließend im McAfee Privacy Service-Bestätigungsdialogfeld auf **OK**.

Benutzeroptionen

Diese Anweisungen gelten nicht für den Administrator.

Sie können Ihr Kennwort und Ihren Benutzernamen ändern. Es empfiehlt sich, Ihr Kennwort zu ändern, nachdem Sie es vom Administrator erhalten haben. Es empfiehlt sich zudem, dass Sie das Kennwort einmal im Monat oder immer dann ändern, wenn Sie denken, dass eine andere Person das Kennwort kennt. Auf diese Weise halten Sie Dritte davon ab, das Internet unter Ihrem Namen zu verwenden.

Ändern Ihres Kennworts

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **McAfee Privacy Service**, und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Kennwort**, und geben Sie Ihr altes Kennwort in das Feld **Altes Kennwort** ein.
3. Geben Sie Ihr neues Kennwort in das Feld **Neues Kennwort** ein.
4. Geben Sie Ihr neues Kennwort erneut in das Feld **Kennwort bestätigen** ein, und klicken Sie anschließend auf **Übernehmen**.
5. Klicken Sie im Bestätigungsdialogfeld auf **OK**. Sie verfügen nun über ein neues Kennwort.

Ändern Ihres Benutzernamens

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **McAfee Privacy Service**, und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Benutzerinformationen**.
3. Geben Sie Ihren neuen Benutzernamen in das Feld **Neuer Benutzername** ein, und klicken Sie anschließend auf **Übernehmen**.
4. Klicken Sie im Bestätigungsdialogfeld auf **OK**. Sie verfügen nun über einen neuen Benutzernamen.

Leeren des Cache

Das Leeren des Cache ist empfehlenswert, da hierdurch verhindert wird, dass ein Kind auf kürzlich von Ihnen besuchte Websites zugreifen kann. Gehen Sie wie folgt vor, um den Cache zu leeren:

1. Öffnen Sie Internet Explorer.
2. Klicken Sie im Menü **Extras** auf **Internetoptionen**. Das Dialogfeld „Internetoptionen“ wird geöffnet.
3. Klicken Sie im Abschnitt **Temporäre Internetdateien** auf **Dateien löschen**. Das Dialogfeld „Dateien löschen“ wird geöffnet.
4. Wählen Sie **Alle Offline-Inhalte löschen**, und klicken Sie anschließend auf **OK**.
5. Klicken Sie nochmals auf **OK**, um das Dialogfeld „Internetoptionen“ zu schließen.

Akzeptieren von Cookies

Die entsprechende Option ist nur verfügbar, wenn Sie vom Administrator befugt sind, Cookies zu akzeptieren oder abzulehnen, wenn diese abgefangen werden.

Wenn Sie auf Websites zugreifen, die Cookies benötigen, können Sie den entsprechenden Seiten den Lesezugriff auf Cookies gewähren.

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **McAfee Privacy Service**, und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Akzeptierte Cookies**.
3. Geben Sie den URL der Website in das Feld **http://** ein, und klicken Sie anschließend auf **Hinzufügen**. Die Website wird in der Liste **Website** angezeigt.

Gehen Sie wie folgt vor, wenn Sie eine Website aus dieser Liste entfernen müssen:

1. Wählen Sie den URL der Website in der Liste **Website** aus.
2. Klicken Sie auf **Entfernen** und anschließend im Bestätigungsdialogfeld auf **Ja**.

Ablehnen von Cookies

Die entsprechende Option ist nur verfügbar, wenn Sie vom Administrator befugt sind, Cookies zu akzeptieren oder abzulehnen, wenn diese abgefangen werden.

Wenn Sie auf Websites zugreifen, die keine Cookies benötigen, können Sie die Cookies ablehnen, ohne eine Aufforderung zu erhalten.

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **McAfee Privacy Service**, und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Abgelehnte Cookies**.
3. Geben Sie den URL der Website in das Feld **http://** ein, und klicken Sie anschließend auf **Hinzufügen**. Die Website wird in der Liste **Website** angezeigt.

Gehen Sie wie folgt vor, wenn Sie eine Website aus dieser Liste entfernen müssen:

1. Wählen Sie den URL der Website in der Liste **Website** aus.
2. Klicken Sie auf **Entfernen** und anschließend im Bestätigungsdialogfeld auf **Ja**.

McAfee SpamKiller 5

Willkommen bei McAfee SpamKiller.

McAfee SpamKiller hilft Ihnen, Ihren E-Mail-Posteingang frei von Spam-E-Mails zu halten. Das Programm umfasst folgende Funktionen:

Funktionen

Diese Version von SpamKiller enthält die folgenden Funktionen:

- Filter: Erweiterte Filteroptionen bieten neue Filtertechniken, einschließlich Unterstützung für Meta-Zeichensatzfilter und Junk-Texterkennung.
- Phishing: Anti-Phishing-Browser-Plugin über eine Internet Explorer-Symbolleiste erkennt und blockiert auf einfache Weise potentielle Phishing-Websites.
- Integration in Microsoft Outlook und Outlook Express: Die Symbolleiste stellt einen Ordner in Ihrem E-Mail-Client bereit, mit dem Sie Spam-Mails direkt blockieren können.
- Installation: schnelle und einfache Einrichtung und Konfiguration. Die automatische Kontenerkennung gewährleistet eine problemlose Einrichtung, Konfiguration und Integration mit vorhandenen E-Mail-Konten.
- Aktualisierungen: Automatische Aktualisierungen werden unauffällig im Hintergrund ausgeführt und sind immer aktiviert, um Ihr Risiko hinsichtlich neu aufgetretener Spam-Bedrohungen zu minimieren.
- Benutzeroberfläche: intuitive Benutzeroberfläche, damit Ihr Computer frei von Spam bleibt.
- Support: Ein kostenloser Instant-Messaging- und E-Mail-Support bietet einen unkomplizierten und umgehenden Live-Kundendienst.

Behandlung von Spam-Nachrichten: Standardmäßig werden Spam-Nachrichten als [SPAM] markiert und in den SpamKiller-Ordner in Outlook und Outlook Express oder in Ihrem Posteingang verschoben. Markierte Nachrichten werden auch auf der Seite „Akzeptierte E-Mails“ angezeigt.

Benutzeroptionen

- Blockieren von Spam-Nachrichten mit Hilfe von Filtern und Speichern von Spam-Nachrichten außerhalb des Posteingangs
- Anzeigen der blockierten und akzeptierten Nachrichten
- Überwachen und Filtern mehrerer E-Mail-Konten
- Importieren der Adressen von Freunden in die Freunde-Liste
- Bekämpfen der Absender von Spam-Mails (Melden von Spam, Versenden von Beschwerden über Absender von Spam-Mails, Erstellen von benutzerdefinierten Filtern)
- Verhindern des Zugriffs auf Spam-Nachrichten durch Kinder
- Blockieren und Wiederherstellen mit einem Mausklick
- Unterstützung für 2-Byte-Zeichensätze (asiatische Sprachen)
- Unterstützung mehrerer Benutzer (unter Windows 2000 und Windows XP)

Filtern

- Automatisches Aktualisieren von Filtern
- Erstellen von benutzerdefinierten Filtern zum Blockieren von E-Mails, die hauptsächlich Bilder, verborgenen Text oder unzulässige Formatierungen enthalten
- Mehrschichtige Kern-Filter-Engine
- Filter für Wörterbuchangriffe
- Adaptives Filtern auf mehreren Ebenen
- Sicherheitsfilter

Erläuterungen zur Symbolleiste

Im oberen Bereich der SpamKiller-Seiten werden die folgenden Symbolschaltflächen angezeigt:

- Durch Klicken auf das Symbol **Benutzer wechseln** können Sie sich unter einem anderen Benutzernamen anmelden.

  Hinweis: Die Schaltfläche **Benutzer wechseln** ist nur dann verfügbar, wenn Sie als Betriebssystem Windows 2000 oder Windows XP verwenden, in SpamKiller mehrere Benutzer hinzugefügt wurden und Sie sich bei SpamKiller als Administrator angemeldet haben.

- Klicken Sie auf **Unterstützung** , um die Online-Support-Seite von McAfee aufzurufen. Hier finden Sie aktuelle Themen zu SpamKiller und anderen McAfee-Produkten, Antworten auf häufig gestellte Fragen und vieles mehr. Sie können nur auf die McAfee-Support-Seite zugreifen, wenn Sie mit dem Internet verbunden sind.
- Klicken Sie auf **Hilfe** , um die Online-Hilfe zu öffnen, die detaillierte Anweisungen zur Einrichtung und Verwendung von SpamKiller enthält.

Wenn SpamKiller auf Ihrem Computer installiert ist, wird in der Taskleiste im Bereich, in dem auch die Systemuhr angegeben ist, das McAfee-Symbol angezeigt. Über dieses McAfee-Symbol können Sie auf SpamKiller, McAfee SecurityCenter und andere auf Ihrem Computer installierte McAfee-Produkte zugreifen.

Deaktivieren von SpamKiller

Sie können SpamKiller deaktivieren und so verhindern, dass E-Mail-Nachrichten gefiltert werden.

So deaktivieren Sie SpamKiller:

Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol , zeigen Sie auf **SpamKiller**, und klicken Sie dann auf **Deaktivieren**. Sie können auch auf die Registerkarte **Zusammenfassung** und dann auf **Klicken Sie zum Deaktivieren hier** klicken.

So aktivieren Sie SpamKiller:

Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **SpamKiller**, und klicken Sie dann auf **Aktivieren**. Sie können auch auf die Registerkarte **Zusammenfassung** und dann auf **Klicken Sie zum Aktivieren hier** klicken.

Erläuterungen zur Seite „Zusammenfassung“

Klicken Sie auf die Registerkarte **Zusammenfassung**, um die Seite „Zusammenfassung“ zu öffnen (Abbildung 5-11).

- Die Option **Übersicht über Ihren SpamKiller-Status** zeigt an, ob der Filter aktiviert wurde, wann die Freunde-Liste zum letzten Mal aktualisiert wurde und wie viele Spam-Nachrichten heute eingegangen sind. Sie können hier den SpamKiller-Filter deaktivieren bzw. aktivieren, die Freunde-Liste aktualisieren und die Registerkarte „Blockierte E-Mails“ öffnen.
- Die Option **Die letzten E-Mails, die als Spam erkannt und blockiert wurden** zeigt die letzten Spam-Nachrichten, die von SpamKiller blockiert und aus dem Posteingang entfernt wurden.
- **E-Mail-Übersicht** zeigt die Gesamtanzahl der E-Mails, die Anzahl der blockierten Spam-Nachrichten und den prozentualen Anteil der Spam-Nachrichten an den gesamten eingegangenen E-Mails an.
- **Neuer Spam** gibt einen Überblick über die Arten von Spam-Nachrichten, die in den letzten 30 Tagen eingegangen sind.

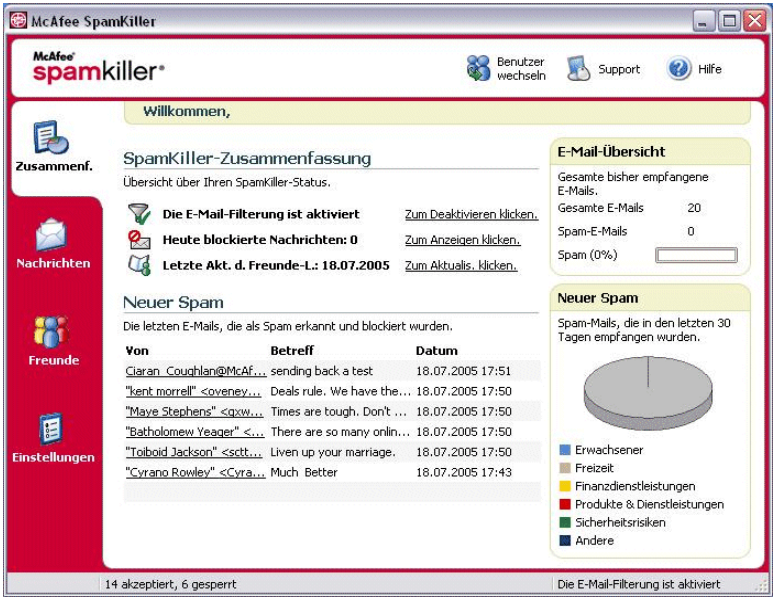


Abbildung 5-11. Seite „Zusammenfassung“

Integration in Microsoft Outlook und Outlook Express

Sie können die Kernfunktionen von SpamKiller über das SpamKiller-Menü oder die SpamKiller-Symbolleiste direkt aus Outlook Express 6.0, Outlook 98, Outlook 2000 und Outlook XP aufrufen.

Die SpamKiller-Symbolleiste wird rechts neben den Standardsymbolleisten in Outlook und Outlook Express angezeigt. Wenn die Symbolleiste nicht angezeigt wird, vergrößern Sie entweder das Fenster des E-Mail-Programms, oder klicken Sie auf die Pfeilsymbole, um weitere Symbolleisten einzublenden.

Wenn die SpamKiller-Symbolleiste zum ersten Mal in Ihrem E-Mail-Programm angezeigt wird, können Sie die Befehle in dieser Symbolleiste nur auf neue Nachrichten anwenden. Bereits im Posteingang vorhandene Spam-Nachrichten müssen manuell gelöscht werden.

Verwalten von E-Mail-Konten und Benutzern

In diesem Abschnitt wird beschrieben, wie Konten und Benutzer verwaltet werden.

Hinzufügen von E-Mail-Konten

Sie können die folgenden E-Mail-Konten hinzufügen:

- Standard-E-Mail-Konto (POP3): Dies ist die am häufigsten verwendete Kontoart.
- MSN/Hotmail-Konto: Webbasierte MSN/Hotmail-Konten

HINWEIS

Wenn Sie Windows 2000 oder Windows XP verwenden und in SpamKiller mehrere Benutzer hinzufügen möchten, müssen Sie diese Benutzer zunächst dem Betriebssystem hinzufügen, bevor Sie ihren Profilen E-Mail-Konten hinzufügen können. Weitere Informationen finden Sie unter *Hinzufügen von Benutzern* auf Seite 119. Wenn Sie in SpamKiller mehrere Benutzer hinzufügen, wird das Konto dem Profil des Benutzers hinzugefügt, der gegenwärtig bei SpamKiller angemeldet ist.

So fügen Sie ein E-Mail-Konto hinzu:

1. Klicken Sie auf die Registerkarte **Einstellungen**, um die Seite „Einstellungen“ zu öffnen (Abbildung 5-12). Klicken Sie anschließend auf **E-Mail-Konten**. Das Dialogfeld **E-Mail-Konten** wird angezeigt, in dem alle in SpamKiller hinzugefügten E-Mail-Konten aufgelistet werden.

   HINWEIS

   Wenn in SpamKiller mehrere Benutzer hinzugefügt wurden, werden in der Liste die E-Mail-Konten des Benutzers angezeigt, der gegenwärtig bei SpamKiller angemeldet ist.

2 Klicken Sie auf **Hinzufügen**. Der Assistent zum Hinzufügen von E-Mail-Konten wird geöffnet.

Befolgen Sie die Anweisungen, die in den Dialogfeldern angezeigt werden.

Wenn Sie ein MSN/Hotmail-Konto hinzufügen, sucht SpamKiller nach einem MSN/Hotmail-Adressbuch, das in Ihre persönlichen Freunde-Liste importiert werden kann.

Abbildung 5-12. Seite „Einstellungen“

Einrichten von E-Mail-Clients für die Verwendung von SpamKiller

Wenn Sie ein Konto hinzugefügt haben, das von SpamKiller nicht entdeckt wurde (das Konto wird nicht im Dialogfeld **Konto auswählen** angezeigt), oder wenn Sie Ihre MSN/Hotmail-E-Mails als POP3-Konto in SpamKiller lesen möchten, müssen Sie Ihren E-Mail-Client für die Verwendung von SpamKiller einrichten, indem Sie den Eintrag für den Posteingangsserver ändern.

Wenn der Eintrag für Ihren Posteingangsserver beispielsweise „mail.mcafee.com“ lautet, ändern Sie ihn in „localhost“.

Löschen von E-Mail-Konten

Sie können die E-Mail-Konten, die von SpamKiller nicht mehr gefiltert werden sollen, aus SpamKiller löschen.

Löschen eines E-Mail-Kontos aus SpamKiller

1 Klicken Sie auf die Registerkarte **Einstellungen**, und wählen Sie **E-Mail-Konten**. Das Dialogfeld **E-Mail-Konten** wird angezeigt, in dem alle in SpamKiller hinzugefügten E-Mail-Konten aufgelistet werden.

> **HINWEIS**
> Wenn in SpamKiller mehrere Benutzer hinzugefügt wurden, werden in der Liste die E-Mail-Konten des Benutzers angezeigt, der gegenwärtig bei SpamKiller angemeldet ist.

2 Wählen Sie ein Konto aus, und klicken Sie dann auf **Löschen**.

Bearbeiten der Eigenschaften von E-Mail-Konten

Die Informationen zu den E-Mail-Konten, die Sie SpamKiller hinzugefügt haben, können jederzeit bearbeitet werden. Zu diesen Informationen gehören beispielsweise die E-Mail-Adresse, die Kontobeschreibung, die Serverinformationen, die Häufigkeit, mit der das Konto von SpamKiller auf Spam-Nachrichten überprüft werden soll, sowie die Art und Weise, wie Ihr Computer mit dem Internet verbunden ist.

POP3-Konten

Bearbeiten von POP3-Konten

1 Klicken Sie auf die Registerkarte **Einstellungen** und dann auf **E-Mail-Konten**. Das Dialogfeld **E-Mail-Konten** wird angezeigt, in dem alle in SpamKiller hinzugefügten E-Mail-Konten aufgelistet werden.

> **HINWEIS**
> Wenn in SpamKiller mehrere Benutzer hinzugefügt wurden, werden in der Liste die E-Mail-Konten des Benutzers angezeigt, der gegenwärtig bei SpamKiller angemeldet ist.

2 Wählen Sie ein POP3-Konto aus, und klicken Sie dann auf **Bearbeiten**.

3 Klicken Sie auf die Registerkarte **Allgemein**, um die Beschreibung und die E-Mail-Adresse des Kontos zu ändern.

- **Beschreibung**: In dieses Feld können Sie einen beliebigen Text eingeben, der das Konto näher beschreibt.
- **E-Mail-Adresse**: Gibt die E-Mail-Adresse des Kontos an.

4 Klicken Sie auf die Registerkarte **Server**, um die Serverinformationen zu bearbeiten.

- **Eingehende E-Mails**: Gibt den Namen des Servers an, der eingehende E-Mails empfängt.
- **Benutzername**: Gibt den Benutzernamen an, den Sie für den Zugriff auf das Konto verwenden. Wird auch als Kontoname bezeichnet.
- **Kennwort**: Gibt das Kennwort an, das Sie für den Zugriff auf das Konto verwenden.
- **Ausgehende E-Mails**: Gibt den Namen des Servers an, der ausgehende E-Mails sendet. Klicken Sie auf **Mehr**, um die Authentifizierungsanforderungen für den Postausgangsserver zu ändern.

5 Klicken Sie auf die Registerkarte **Überprüfung**, wenn Sie die Häufigkeit ändern möchten, mit der das Konto von SpamKiller auf Spam-Nachrichten überprüft werden soll:

a Aktivieren Sie entweder **Überprüfen alle** oder **Täglich prüfen um**, und wählen Sie dann im zugehörigen Feld eine Zeit aus bzw. geben diese ein. Wenn Sie Null eingeben, wird das Konto nur beim Herstellen einer Verbindung von SpamKiller überprüft.

b Geben Sie an, bei welchen weiteren Gelegenheiten das Konto von SpamKiller gefiltert werden soll:

Beim Starten prüfen: Aktivieren Sie diese Option, wenn Ihr Computer über eine Direktverbindung verfügt und das Konto bei jedem Starten des Computers von SpamKiller überprüft werden soll.

Überprüfen, wenn eine Einwahlverbindung hergestellt wird: Aktivieren Sie diese Option, wenn Ihr Computer über eine Einwahlverbindung verbunden wird und das Konto bei jeder Einwahl von SpamKiller überprüft werden soll.

6 Klicken Sie auf die Registerkarte **Verbindung**, wenn Sie festlegen möchten, wie SpamKiller eine Internetverbindung herstellen soll, damit neu eingegangene Nachrichten in Ihrem Posteingang überprüft werden können.

- **Nie eine Einwahlverbindung herstellen**: SpamKiller stellt keine automatischen Verbindungen her. Sie müssen Ihre Einwahlverbindung zuerst manuell starten.
- **Bei Bedarf wählen**: Wenn keine Internetverbindung verfügbar ist, versucht SpamKiller automatisch, mit Hilfe der Standard-Einwahlverbindung im DFÜ-Netzwerk eine Verbindung herzustellen.
- **Immer wählen**: SpamKiller versucht automatisch, mit Hilfe der von Ihnen angegebenen Einwahlverbindung eine Verbindung herzustellen.
- **Verbindung beibehalten, nachdem die erste Filterung ausgeführt wurde**: Die Verbindung mit dem Internet bleibt nach dem Filtern bestehen.

7 Klicken Sie auf die Registerkarte **Erweitert**, um die erweiterten Optionen zu bearbeiten.

- **Spam-Meldungen auf dem Server lassen**: Aktivieren Sie diese Option, wenn auf Ihrem E-Mail-Server eine Kopie der blockierten Nachrichten gespeichert werden soll. Sie können diese E-Mails sowohl vom E-Mail-Client aus als auch auf der SpamKiller-Seite „Blockierte E-Mails“ anzeigen. Wenn das Kontrollkästchen nicht aktiviert ist, können blockierte Nachrichten nur auf der Seite „Blockierte E-Mails“ angezeigt werden.
- **POP3-Anschluss**: Die Nummer des POP3-Anschlusses. Der POP3-Server ist der Server, der die eingehenden Nachrichten bearbeitet.
- **SMTP-Anschluss**: Die Nummer des SMTP-Anschlusses. Der SMTP-Server ist der Server, der die ausgehenden Nachrichten bearbeitet.
- **Server-Zeitüberschreitung**: Gibt an, wie lange SpamKiller bei Inaktivität auf den Eingang von E-Mails wartet, bis eine Zeitüberschreitung eintritt und das Programm angehalten wird.

  Erhöhen Sie den Wert für die Server-Zeitüberschreitung, falls Sie beim Abrufen der E-Mails Probleme haben. Eine mögliche Ursache könnte eine zu langsame E-Mail-Verbindung sein, so dass aufgrund der Erhöhung des Wertes SpamKiller länger wartet, bevor die Zeitüberschreitung eintritt.

8 Klicken Sie auf **OK**.

MSN/Hotmail-Konten

Bearbeiten von MSN/Hotmail-Konten

1 Klicken Sie auf die Registerkarte **Einstellungen** und dann auf **E-Mail-Konten**.

Das Dialogfeld **E-Mail-Konten** wird angezeigt, in dem alle in SpamKiller hinzugefügten E-Mail-Konten aufgelistet werden.

> **HINWEIS**
> Wenn in SpamKiller mehrere Benutzer hinzugefügt wurden, werden in der Liste die E-Mail-Konten des Benutzers angezeigt, der gegenwärtig bei SpamKiller angemeldet ist.

2 Wählen Sie ein MSN/Hotmail-Konto aus, und klicken Sie dann auf **Bearbeiten**.

3 Klicken Sie auf die Registerkarte **Allgemein**, um die Beschreibung und die E-Mail-Adresse des Kontos zu ändern.

- **Beschreibung**: In dieses Feld können Sie einen beliebigen Text eingeben, der das Konto näher beschreibt.
- **E-Mail-Adresse**: Gibt die E-Mail-Adresse des Kontos an.

4 Klicken Sie auf die Registerkarte **Server**, um die Serverinformationen zu bearbeiten.

- **Eingehende E-Mails**: Gibt den Namen des Servers an, der eingehende E-Mails empfängt.
- **Kennwort**: Gibt das Kennwort an, das Sie für den Zugriff auf das Konto verwenden.
- **Ausgehende E-Mails**: Gibt den Namen des Servers an, der ausgehende E-Mails sendet.
- **SMTP-Server für ausgehende E-Mails verwenden**: Aktivieren Sie diese Option, wenn Sie Fehlermeldungen senden, die MSN-Signaturzeile jedoch nicht in die Fehlermeldung aufnehmen möchten. Wenn die MSN-Signaturzeile enthalten ist, können Absender von Spam-Mails leicht erkennen, dass es sich bei der Fehlermeldung um eine falsche Fehlermeldung handelt.

  Klicken Sie auf **Mehr**, um die Authentifizierungsanforderungen für den Postausgangsserver zu ändern.

5 Klicken Sie auf die Registerkarte **Überprüfung**, wenn Sie die Häufigkeit ändern möchten, mit der das Konto von SpamKiller auf Spam-Nachrichten überprüft werden soll:

a Aktivieren Sie entweder **Überprüfen alle** oder **Täglich prüfen um**, und wählen Sie dann im zugehörigen Feld eine Zeit aus bzw. geben diese ein. Wenn Sie Null eingeben, wird das Konto nur beim Herstellen einer Verbindung von SpamKiller überprüft.

b Geben Sie an, bei welchen weiteren Gelegenheiten das Konto von SpamKiller gefiltert werden soll:

Beim Starten prüfen: Aktivieren Sie diese Option, wenn Ihr Computer über eine Direktverbindung verfügt und das Konto bei jedem Starten von SpamKiller überprüft werden soll.

Überprüfen, wenn eine Einwahlverbindung hergestellt wird: Aktivieren Sie diese Option, wenn Ihr Computer über eine Einwahlverbindung verbunden wird und das Konto bei jeder Einwahl von SpamKiller überprüft werden soll.

6 Klicken Sie auf die Registerkarte **Verbindung**, wenn Sie festlegen möchten, wie SpamKiller eine Internetverbindung herstellen soll, damit neu eingegangene Nachrichten in Ihrem Posteingang überprüft werden können.

- **Nie eine Einwahlverbindung herstellen**: SpamKiller stellt keine automatischen Verbindungen her. Sie müssen Ihre Einwahlverbindung zuerst manuell starten.

- **Bei Bedarf wählen**: Wenn keine Internet-Verbindung verfügbar ist, versucht SpamKiller automatisch, mit Hilfe der Standard-Einwahlverbindung im DFÜ-Netzwerk eine Verbindung herzustellen.
- **Immer wählen**: SpamKiller versucht automatisch, mit Hilfe der von Ihnen angegebenen Einwahlverbindung eine Verbindung herzustellen.
- **Verbindung beibehalten, nachdem die erste Filterung ausgeführt wurde**: Die Verbindung mit dem Internet bleibt nach dem Filtern bestehen.

7 Klicken Sie auf **OK**.

Konfigurieren von Hotmail-Konten, um Spam in Outlook oder Outlook Express zu blockieren

SpamKiller kann Hotmail-Konten direkt filtern. Weitere Informationen dazu finden Sie in der Online-Hilfe. Bevor Sie jedoch die SpamKiller-Symbolleiste in Outlook oder Outlook Express zum Blockieren von Nachrichten oder Hinzufügen von Freunden verwenden können, müssen Sie Ihr Hotmail-Konto entsprechend konfigurieren.

1 Konfigurieren Sie Ihr Hotmail-Konto in MSK.

2 Sie müssen bereits vorhandene Hotmail-Konten in Outlook oder Outlook Express zuerst entfernen.

3 Fügen Sie Ihr Hotmail-Konto in Outlook oder Outlook Express hinzu. Stellen Sie sicher, dass für den Typ des Kontos und des Posteingangsservers **POP3** ausgewählt ist.

4 Legen Sie für den Posteingangsserver den Namen **`localhost`** fest.

5 Geben Sie den Namen für den Postausgangsserver (SMTP-Server) ein (obligatorisch).

6 Schließen Sie den Kontokonfigurationsvorgang ab. Sie können jetzt neue Hotmail-Spam-Nachrichten filtern oder Freunde zur Freunde-Liste hinzufügen.

MAPI-Konten

Für eine erfolgreiche SpamKiller-MAPI-Integration in Outlook müssen die folgenden Voraussetzungen erfüllt werden:

- Outlook wurde ursprünglich mit Unternehmens- und Arbeitsgruppenunterstützung installiert (nur Outlook 98).
- Das erste E-Mail-Konto ist ein MAPI-Konto (nur Outlook 98).
- Der Computer ist bei der Domäne angemeldet.

Bearbeiten von MAPI-Konten

1. Klicken Sie auf die Registerkarte **Einstellungen** und dann auf **E-Mail-Konten**. Das Dialogfeld **E-Mail-Konten** wird angezeigt, in dem alle in SpamKiller hinzugefügten E-Mail-Konten aufgelistet werden.

   HINWEIS
   Wenn in SpamKiller mehrere Benutzer hinzugefügt wurden, werden in der Liste die E-Mail-Konten des Benutzers angezeigt, der gegenwärtig bei SpamKiller angemeldet ist.

2. Wählen Sie ein MAPI-Konto aus, und klicken Sie dann auf **Bearbeiten**.

3. Klicken Sie auf die Registerkarte **Allgemein**, um die Beschreibung und die E-Mail-Adresse des Kontos zu ändern.

   - **Beschreibung**: In dieses Feld können Sie einen beliebigen Text eingeben, der das Konto näher beschreibt.
   - **E-Mail-Adresse**: Gibt die E-Mail-Adresse des Kontos an.

4. Klicken Sie auf die Registerkarte **Profil**, wenn Sie die Profilinformationen bearbeiten möchten.

   - **Profil**: Gibt das MAPI-Profil für das Konto an.
   - **Kennwort**: Gibt das Kennwort an, das dem MAPI-Profil entspricht, sofern ein solches eingerichtet wurde (nicht notwendigerweise das Kennwort für das E-Mail-Konto).

5. Klicken Sie auf die Registerkarte **Verbindung**, wenn Sie festlegen möchten, wie SpamKiller eine Internetverbindung herstellen soll, damit neu eingegangene Nachrichten in Ihrem Posteingang überprüft werden können:

   - **Nie eine Einwahlverbindung herstellen**: SpamKiller stellt keine automatischen Verbindungen her. Sie müssen Ihre Einwahlverbindung zuerst manuell starten.
   - **Bei Bedarf wählen**: Wenn keine Internet-Verbindung verfügbar ist, versucht SpamKiller automatisch, mit Hilfe der Standard-Einwahlverbindung im DFÜ-Netzwerk eine Verbindung herzustellen.
   - **Immer wählen**: SpamKiller versucht automatisch, mit Hilfe der von Ihnen angegebenen Einwahlverbindung eine Verbindung herzustellen.
   - **Verbindung beibehalten, nachdem die erste Filterung ausgeführt wurde**: Die Verbindung mit dem Internet bleibt nach dem Filtern bestehen.

6. Klicken Sie auf **OK**.

Hinzufügen von Benutzern

SpamKiller unterstützt die Einrichtung von mehreren Benutzern, die den im Betriebssystem (Windows 2000 bzw. Windows XP) eingerichteten Benutzern entsprechen.

Bei der Installation von SpamKiller wird automatisch ein Administrator-Benutzerprofil für den Benutzer erstellt, der zum Zeitpunkt der Installation angemeldet war. Wenn Sie während der Installation E-Mail-Konten in SpamKiller hinzufügen, werden diese dem Administrator-Benutzerprofil zugeordnet.

Bevor Sie in SpamKiller weitere E-Mail-Konten hinzufügen, sollten Sie feststellen, ob Sie weitere SpamKiller-Benutzer hinzufügen müssen. Das Hinzufügen von Benutzern kann von Vorteil sein, wenn Ihr Computer von mehreren Benutzern verwendet wird, die alle jeweils über ein eigenes E-Mail-Konto verfügen. Die E-Mail-Konten der Benutzer werden dem jeweiligen Benutzerprofil hinzugefügt, so dass die Benutzer selbst ihre E-Mail-Konten, ihre persönlichen Einstellungen, ihre persönlichen Filter und die Liste ihrer persönlichen Freunde verwalten können.

Es hängt vom Benutzertyp ab, welche Aufgaben der Benutzer in SpamKiller ausführen kann. Die folgende Tabelle gibt Ihnen einen Überblick über die Zugriffsrechte der zwei Benutzertypen. Administratoren können alle Aufgaben ausführen, während Benutzer mit eingeschränkten Rechten nur Aufgaben ausführen können, die ihrem persönlichen Profil entsprechen. Beispielsweise können Administratoren den gesamten Inhalt von blockierten Nachrichten anzeigen, während Benutzer mit eingeschränkten Rechten nur die Betreffzeilen anzeigen können.

Tasks	Administrator	Benutzer mit eingeschränkten Rechten
Verwalten der persönlichen E-Mail-Konten, der persönlichen Filter, der persönlichen Freunde-Liste und der persönlichen Audioeinstellungen	X	X
Verwalten der persönlichen Seiten „Blockierte E-Mails“ und „Akzeptierte E-Mails“	X	X
Anzeigen des Inhalts blockierter Nachrichten	X	
Anzeigen des Inhalts akzeptierter Nachrichten	X	X
Verwalten der allgemeinen Filter und der allgemeinen Freunde-Liste	X	
Melden von Spam an McAfee	X	X
Senden von Beschwerden und Fehlermeldungen	X	X

Tasks	Administrator	Benutzer mit eingeschränkten Rechten
Verwalten von Beschwerden und Fehlermeldungen (Erstellen, Bearbeiten und Löschen von Meldungsvorlagen)	X	
Verwalten von Benutzern (Erstellen, Bearbeiten und Entfernen von Benutzern)	X	
Sichern und Wiederherstellen von SpamKiller	X	
Anzeigen der Zusammenfassung der empfangenen Spam-Nachrichten	X	X

Wenn sich ein gerade hinzugefügter Benutzer an Ihrem Computer anmeldet, wird er dazu aufgefordert, ein E-Mail-Konto zu seinem Benutzerprofil hinzuzufügen.

Folgende Bedingungen müssen zum Hinzufügen und Verwalten von Benutzern erfüllt werden:

- Sie müssen bei SpamKiller als Administrator angemeldet sein.
- Auf Ihrem Computer muss Windows 2000 oder Windows XP ausgeführt werden.
- Die Benutzer, die hinzugefügt bzw. verwaltet werden sollen, müssen über Windows-Benutzerkonten verfügen.

Benutzerkennwörter und Kinderschutz vor Spam

Durch das Erstellen eines Benutzerkennworts wird der Schutz vor Datenmissbrauch erhöht. Ohne das Anmeldekennwort kann kein anderer Benutzer auf die persönlichen Einstellungen, die Freunde-Liste und die Liste der akzeptierten E-Mails zugreifen. Mit Kennwörtern lässt sich auch verhindern, dass Kinder ungehinderten Zugang zu SpamKiller erhalten und den Inhalt von Spam-Nachrichten lesen.

Erstellen eines Kennworts für einen bereits eingerichteten SpamKiller-Benutzer

1. Klicken Sie auf die Registerkarte **Einstellungen** und dann auf **Benutzer**.
2. Wählen Sie einen Benutzer aus, und klicken Sie dann auf **Bearbeiten**.
3. Geben Sie im Feld **Kennwort** das Kennwort ein. Wenn der Benutzer auf SpamKiller zugreifen möchte, muss er das Kennwort eingeben, um sich anmelden zu können.

WICHTIG
Es gibt keine Möglichkeit, ein vergessenes Kennwort abzurufen. Ein neues Kennwort kann nur von einem SpamKiller-Administrator erstellt werden.

Hinzufügen von Benutzern in SpamKiller

1 Klicken Sie auf die Registerkarte **Einstellungen** und dann auf **Benutzer**.

2 Klicken Sie auf **Hinzufügen**.

Es wird eine Liste der Windows-Benutzer angezeigt. Wenn Sie einen Benutzer hinzufügen möchten, der nicht in der Liste angezeigt wird, erstellen Sie ein Windows-Benutzerkonto für ihn. Dann muss sich der neue Benutzer mindestens einmal an Ihrem Computer anmelden. Danach können Sie den Benutzer in SpamKiller hinzufügen.

HINWEIS
Windows-Benutzer mit Administratorrechten verfügen auch über SpamKiller-Administratorrechte.

3 Wählen Sie einen hinzuzufügenden Benutzer aus, und klicken Sie dann auf **OK**. Der Benutzer wird daraufhin in SpamKiller hinzugefügt und in der Liste der SpamKiller-Benutzer angezeigt.

4 Klicken Sie nach dem Hinzufügen von Benutzern auf **Schließen**.

Informationen zum Erstellen eines Kennworts für einen Benutzer finden Sie unter *Erstellen eines Kennworts für einen bereits eingerichteten SpamKiller-Benutzer* auf Seite 120.

Wenn sich der Benutzer das nächste Mal bei SpamKiller anmeldet, wird er aufgefordert, seinem SpamKiller-Benutzerprofil ein E-Mail-Konto hinzuzufügen. Sie können dem Benutzerprofil E-Mail-Konten hinzufügen, wenn Sie als Benutzer bei SpamKiller angemeldet sind und über die entsprechenden Informationen zum E-Mail-Konto verfügen. Einzelheiten dazu finden Sie unter *Hinzufügen von E-Mail-Konten* auf Seite 111.

Bearbeiten von SpamKiller-Benutzerprofilen

1 Klicken Sie auf die Registerkarte **Einstellungen** und dann auf **Benutzer**. Eine Liste der SpamKiller-Benutzer wird eingeblendet.

2 Wählen Sie einen Benutzer aus, und klicken Sie dann auf **Bearbeiten**.

3 Geben Sie einen neuen Namen und ein neues Kennwort ein.

Löschen von SpamKiller-Benutzerprofilen

WARNUNG
Wenn Sie ein Benutzerprofil löschen, werden auch die E-Mail-Konten dieses Benutzers aus SpamKiller entfernt.

1. Klicken Sie auf die Registerkarte **Einstellungen** und dann auf **Benutzer**. Eine Liste der SpamKiller-Benutzer wird eingeblendet.
2. Wählen Sie den zu löschenden Benutzer aus, und klicken Sie dann auf **Löschen**.

Anmelden bei SpamKiller auf einem Computer mit mehreren Benutzern

Wenn sich Benutzer an Ihrem Computer anmelden und SpamKiller öffnen, werden Sie automatisch entsprechend ihrem Benutzerprofil bei SpamKiller angemeldet. Wenn SpamKiller-Kennwörter für die Benutzer eingerichtet wurden, müssen sie das jeweilige Kennwort im Dialogfeld **Anmelden** eingeben.

Wechseln zwischen Benutzern

Sie müssen bei SpamKiller als Administrator angemeldet sein.

1. Klicken Sie im oberen Bereich der Seite auf **Benutzer wechseln**. Das Dialogfeld **Benutzer wechseln** wird geöffnet.
2. Wählen Sie einen Benutzer aus, und klicken Sie auf **OK**. Wenn der Benutzer über ein Kennwort verfügt, wird das Dialogfeld **Anmelden** angezeigt. Geben Sie im Feld **Kennwort** das Benutzerkennwort ein, und klicken Sie dann auf **OK**.

Verwenden der Freunde-Liste

Wir empfehlen, die Namen Ihrer Freunde und deren E-Mail-Adressen in eine Freunde-Liste einzutragen. Nachrichten, die von Adressen aus dieser Liste stammen, werden von SpamKiller nicht blockiert. Wenn Sie eine solche Liste erstellen, wird sichergestellt, dass SpamKiller erwünschte Nachrichten akzeptiert und passieren lässt.

Sie können in SpamKiller Namen, E-Mail-Adressen, Domänen und Mailing-Listen zur Freunde-Liste hinzufügen. Sie können entweder eine einzelne Adresse oder alle Adressen auf einmal hinzufügen, indem Sie ein Adressbuch aus Ihrem E-Mail-Programm importieren.

SpamKiller kennt zwei Arten von Listen:

- **Allgemeine Freunde-Liste**: Diese Liste wirkt sich auf alle E-Mail-Konten für die Benutzer in SpamKiller aus. Wenn Sie mehrere Benutzer hinzugefügt haben, müssen Sie sich bei SpamKiller als Administrator anmelden, um die allgemeine Freunde-Liste verwalten zu können.
- **Persönliche Freunde-Liste**: Diese Liste wirkt sich auf alle E-Mail-Konten eines bestimmten Benutzers in SpamKiller aus. Wenn Sie mehrere Benutzer hinzugefügt haben, müssen Sie sich bei SpamKiller als der entsprechende Benutzer anmelden, um die persönliche Freunde-Liste verwalten zu können.

Sie können der Freunde-Liste Adressen von Freunden hinzufügen und so sicherstellen, dass E-Mails von diesen Adressen nicht blockiert werden. Auf der Seite „Freunde“ werden die Namen und Adressen der Personen angezeigt, die Sie der Freunde-Liste hinzugefügt haben. Für jeden Eintrag in der Freunde-Liste wird zusätzlich das Datum der Aufnahme in die Liste sowie die Gesamtzahl der von dieser Adresse empfangenen Nachrichten angezeigt.

Klicken Sie auf die Registerkarte **E-Mail-Adressen**, um die E-Mail-Adressen in der Freunde-Liste anzuzeigen. Klicken Sie auf die Registerkarte **Domänen**, um die Domänenadressen in der Freunde-Liste anzuzeigen. Klicken Sie auf die Registerkarte **Mailing-Listen**, um die Mailing-Listen in der Freunde-Liste anzuzeigen.

Sie können von der allgemeinen zur persönlichen Freunde-Liste wechseln, indem Sie auf der Registerkarte **E-Mail-Adresse**, **Domänen** oder **Mailing-Listen** auf die Schaltfläche mit dem nach unten zeigenden Pfeil klicken und dann **Persönliche Freunde-Liste** auswählen.

Öffnen einer Freunde-Liste

1 Zum Öffnen einer Freunde-Liste klicken Sie auf die Registerkarte **Freunde**. Die Seite „Freunde“ wird eingeblendet (Abbildung 5-13).

2 Klicken Sie auf die Registerkarte **E-Mail-Adresse**, **Domänen** oder **Mailing-Liste**. Die allgemeine Freunde-Liste wird angezeigt. Wenn Sie Ihre persönliche Freunde-Liste anzeigen möchten, klicken Sie auf einer der Registerkarten auf den nach unten zeigenden Pfeil und wählen Sie dann **Persönliche Freunde-Liste** aus.

HINWEIS
Wenn Sie Windows 2000 oder Windows XP verwenden und in SpamKiller mehrere Benutzer hinzugefügt haben, können Benutzer mit eingeschränkten Rechten nur auf ihre persönliche Freunde-Liste zugreifen.

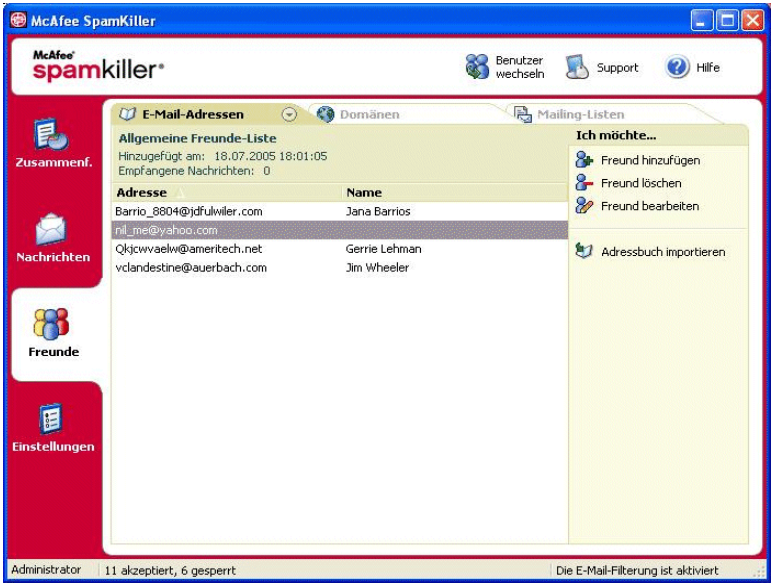


Abbildung 5-13. Seite „Freunde“

Importieren von Adressbüchern

Adressbücher können manuell oder automatisch in eine Freunde-Liste importiert werden. Beim automatischen Import kann SpamKiller Ihre Adressbücher regelmäßig auf neue Adressen überprüfen und diese automatisch in eine Freunde-Liste importieren.

Adressbücher können aus den folgenden E-Mail-Programmen importiert werden:

- Microsoft Outlook (ab Version 98)
- Microsoft Outlook Express (alle Versionen)
- Netscape Communicator (Version 6 und vorherige Versionen, wenn Adressbücher als LDIF-Datei exportiert wurden)
- Qualcomm Eudora (ab Version 5)
- IncrediMail Xe
- MSN/Hotmail
- Alle Programme, die ihre Adressbücher als reine Textdatei exportieren können

Automatisches Importieren von Adressbüchern

Sie können Ihre persönliche Freunde-Liste regelmäßig aktualisieren, indem Sie einen Zeitplan für das automatische Importieren von Adressen aus den Adressbüchern erstellen.

1. Klicken Sie auf die Registerkarte **Einstellungen** und dann auf **Adressbücher**. Das Dialogfeld **Adressbücher importieren** wird angezeigt, in dem eine Liste mit Adressbüchern enthalten ist, die SpamKiller regelmäßig überprüft und aus der es neue Adressen importiert.
2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Zeitplan importieren** wird angezeigt.
3. Wählen Sie unter **Typ** den Typ des zu importierenden Adressbuches und unter **Quelle** die Quelle für das Adressbuch aus.
4. Legen Sie im Feld **Planen** fest, wie oft SpamKiller das Adressbuch nach neuen Adressen durchsuchen soll.
5. Klicken Sie auf **OK**. Nach einer Aktualisierung werden die neuen Adressen in der persönlichen Freunde-Liste angezeigt.

Manuelles Importieren von Adressbüchern

Sie können Adressbücher sowohl in Ihre persönliche Freunde-Liste als auch in die allgemeine Freunde-Liste manuell importieren.

HINWEIS
Wenn Sie Windows 2000 oder Windows XP verwenden und in SpamKiller mehrere Benutzer hinzugefügt haben, müssen Sie sich bei SpamKiller als Administrator anmelden, um der allgemeinen Freunde-Liste Adressen von Freunden hinzufügen zu können.

1. Klicken Sie auf die Registerkarte **Freunde** und dann auf **Adressbuch importieren**.

   Das Dialogfeld **Adressbuch importieren** wird angezeigt, in dem eine Liste der Adressbuchtypen enthalten ist, die importiert werden können.

2. Wählen Sie den Typ des zu importierenden Adressbuches aus oder klicken Sie auf **Durchsuchen**, um die in einer Datei gespeicherten Adressen zu importieren.

   Um das Adressbuch in Ihre persönliche Freunde-Liste zu importieren, stellen Sie sicher, dass das Kontrollkästchen **In die Liste der persönlichen Freunde hinzufügen** aktiviert ist. Wenn Sie das Adressbuch in die allgemeine Freunde-Liste importieren möchten, vergewissern Sie sich, dass das Kontrollkästchen nicht aktiviert ist.

3. Klicken Sie auf **Weiter**. Auf einer Bestätigungsseite wird die Anzahl der Adressen angezeigt, die von SpamKiller hinzugefügt wurden.

4. Klicken Sie auf **Fertig stellen**. Die Adressen werden nun in der allgemeinen Freunde-Liste bzw. der persönlichen Freunde-Liste angezeigt.

Bearbeiten von Adressbuchinformationen

Sie können Informationen für automatisch importierte Adressbücher bearbeiten.

1. Klicken Sie auf die Registerkarte **Einstellungen** und dann auf **Adressbücher**.
2. Wählen Sie ein Adressbuch aus, und klicken Sie dann auf **Bearbeiten**.
3. Bearbeiten Sie die Adressbuchinformationen, und klicken Sie dann auf **OK**.

Löschen von Adressbüchern aus der Liste der automatisch importierten Adressbücher

Wenn SpamKiller keine Adressen mehr automatisch aus einem Adressbuch importieren soll, löschen Sie den entsprechenden Adressbucheintrag.

1. Klicken Sie auf die Registerkarte **Einstellungen** und dann auf **Adressbücher**.
2. Wählen Sie ein Adressbuch aus, und klicken Sie dann auf **Löschen**. Ein Bestätigungsdialogfeld wird eingeblendet.
3. Klicken Sie auf **Ja**, um das Adressbuch aus der Liste zu entfernen.

Hinzufügen von Freunden

Wenn Sie sicherstellen möchten, dass Sie alle E-Mails von Ihren Freunden erhalten, fügen Sie die Namen und Adressen Ihrer Freunde einer Freunde-Liste hinzu. Freunde können über die Seite „Freunde“, die Registerkarten „Blockierte E-Mails“ und „Akzeptierte E-Mails“ sowie aus Microsoft Outlook oder Outlook Express hinzugefügt werden.

HINWEIS
Wenn Sie Windows 2000 oder Windows XP verwenden und in SpamKiller mehrere Benutzer hinzugefügt haben, müssen Sie sich bei SpamKiller als Administrator anmelden, um der allgemeinen Freunde-Liste Adressen von Freunden hinzufügen zu können.

Hinzufügen von Freunden über die Registerkarte „Blockierte E-Mails“ oder „Akzeptierte E-Mails“

1. Klicken Sie auf die Registerkarte **Nachrichten** und dann auf die Registerkarte **Blockierte E-Mails** bzw. **Akzeptierte E-Mails**.

   Oder

   Wählen Sie im SpamKiller-Menü in Microsoft Outlook oder Outlook Express die Option **Blockierte Meldungen anzeigen**, um die Registerkarte „Blockierte E-Mails“ für dieses Konto anzuzeigen.

   Die Registerkarte „Blockierte E-Mails“ bzw. „Akzeptierte E-Mails“ wird geöffnet.

2. Wählen Sie eine Nachricht von einem Absender, den Sie einer Freunde-Liste hinzufügen möchten, und klicken Sie dann auf **Freund hinzufügen**.

3. Geben Sie im Feld **Adresse** die Adresse ein, die Sie der Freunde-Liste hinzufügen möchten. Das Feld **Adresse** kann bereits die Adresse der ausgewählten Nachricht enthalten.

4. Geben Sie im Feld **Name** den Namen des Freundes ein.

5. Wählen Sie im Feld **Freundestyp** den Typ der Adresse aus, die Sie hinzufügen möchten:

   - **Einzelne E-Mail-Adresse**: Die E-Mail-Adresse des Absenders wird dem Bereich „Domänen“ in der Freunde-Liste hinzugefügt.
   - **Alle in einer Domäne**: Der Domänenname wird dem Bereich **Domänen** in der Freunde-Liste hinzugefügt. SpamKiller akzeptiert dann alle E-Mails, die von dieser Domäne eingehen.
   - **Mailing-Liste**: Die Adresse wird dem Bereich **Mailing-Liste** in der Freunde-Liste hinzugefügt.

Wenn Sie die Adresse nur Ihrer persönlichen Freunde-Liste hinzufügen möchten, vergewissern Sie sich, dass das Kontrollkästchen **In die Liste der persönlichen Freunde hinzufügen** aktiviert ist. Um die Adresse nur der allgemeinen Freunde-Liste hinzuzufügen, vergewissern Sie sich, dass das Kontrollkästchen nicht aktiviert ist.

6 Klicken Sie auf **OK**. Alle Nachrichten von dieser Adresse werden als Nachrichten von einem Freund gekennzeichnet und auf der Seite „Akzeptierte E-Mails“ angezeigt.

Hinzufügen von Freunden über die Seite „Freunde“

1 Klicken Sie auf die Registerkarte **Freunde** und dann auf **Freund hinzufügen**. Das Dialogfeld **Freund-Eigenschaften** wird geöffnet.

2 Geben Sie im Feld **Adresse** die Adresse ein, die Sie der Freunde-Liste hinzufügen möchten.

3 Geben Sie im Feld **Name** den Namen des Freundes ein.

4 Wählen Sie im Feld **Freundestyp** den Typ der Adresse aus, die Sie hinzufügen möchten:

- **Einzelne E-Mail-Adresse**: Die E-Mail-Adresse des Absenders wird dem Bereich „Domänen“ in der Freunde-Liste hinzugefügt.
- **Alle in einer Domäne**: Der Domänenname wird dem Bereich **Domänen** in der Freunde-Liste hinzugefügt. SpamKiller akzeptiert dann alle E-Mails, die von dieser Domäne eingehen.
- **Mailing-Liste**: Die Adresse wird dem Bereich **Mailing-Liste** in der Freunde-Liste hinzugefügt.

Wenn Sie die Adresse nur Ihrer persönlichen Freunde-Liste hinzufügen möchten, vergewissern Sie sich, dass das Kontrollkästchen **In die Liste der persönlichen Freunde hinzufügen** aktiviert ist. Um die Adresse nur der allgemeinen Freunde-Liste hinzuzufügen, vergewissern Sie sich, dass das Kontrollkästchen nicht aktiviert ist.

5 Klicken Sie auf **OK**. Alle Nachrichten von dieser Adresse werden als Nachrichten von einem Freund gekennzeichnet und auf der Seite „Akzeptierte E-Mails“ angezeigt.

Hinzufügen von Freunden über Microsoft Outlook:

1 Öffnen Sie Ihr E-Mail-Konto in Microsoft Outlook oder Outlook Express.

2 Wählen Sie eine Nachricht von einem Absender, den Sie einer Freunde-Liste hinzufügen möchten.

3 Klicken Sie in der Microsoft Outlook-Symbolleiste auf das Symbol . Alle Nachrichten von dieser Adresse werden als Nachrichten von einem Freund gekennzeichnet und auf der Seite „Akzeptierte E-Mails“ angezeigt.

Bearbeiten von Einträgen in den Freunde-Listen

1 Klicken Sie auf die Registerkarte **Freunde** und dann auf die Registerkarte **E-Mail-Adresse**, **Domänen** oder **Mailing-Liste**.

Die allgemeine Freunde-Liste wird angezeigt. Wenn Sie Ihre persönliche Freunde-Liste anzeigen möchten, klicken Sie auf einer der Registerkarten auf den nach unten zeigenden Pfeil und wählen Sie dann **Persönliche Freunde-Liste** aus.

HINWEIS
Wenn Sie Windows 2000 oder Windows XP verwenden und in SpamKiller mehrere Benutzer hinzugefügt haben, können nur Benutzer mit Administratorrechten auf die allgemeine Freunde-Liste zugreifen.

2 Wählen Sie in der Liste eine Adresse aus, und klicken Sie dann auf **Bearbeiten**.
3 Bearbeiten Sie die entsprechenden Informationen, und klicken Sie dann auf **OK**.

Löschen von Freunde-Einträgen

Entfernen Sie Adressen, die Sie nicht mehr benötigen, aus der Freunde-Liste.

1 Klicken Sie auf die Registerkarte **Freunde** und dann auf die Registerkarte **E-Mail-Adresse**, **Domänen** oder **Mailing-Liste**.

Die allgemeine Freunde-Liste wird angezeigt. Wenn Sie Ihre persönliche Freunde-Liste anzeigen möchten, klicken Sie auf einer der Registerkarten auf den nach unten zeigenden Pfeil und wählen Sie dann **Persönliche Freunde-Liste** aus.

HINWEIS
Wenn Sie Windows 2000 oder Windows XP verwenden und in SpamKiller mehrere Benutzer hinzugefügt haben, können nur Benutzer mit Administratorrechten auf die allgemeine Freunde-Liste zugreifen.

2 Wählen Sie in der Liste eine Adresse aus, und klicken Sie dann auf **Freund löschen**.

3 Klicken Sie auf **Ja**, um diesen Eintrag aus der Freunde-Liste zu entfernen.

Arbeiten mit blockierten und akzeptierten Nachrichten

Klicken Sie auf die Registerkarte **Nachrichten**, um die Seite „Nachrichten“ zu öffnen (Abbildung 5-14). Sie können dort auf die blockierten und akzeptierten Nachrichten zugreifen. Die Registerkarten „Blockierte E-Mails“ und „Akzeptierte E-Mails“ sind im Wesentlichen gleich strukturiert.

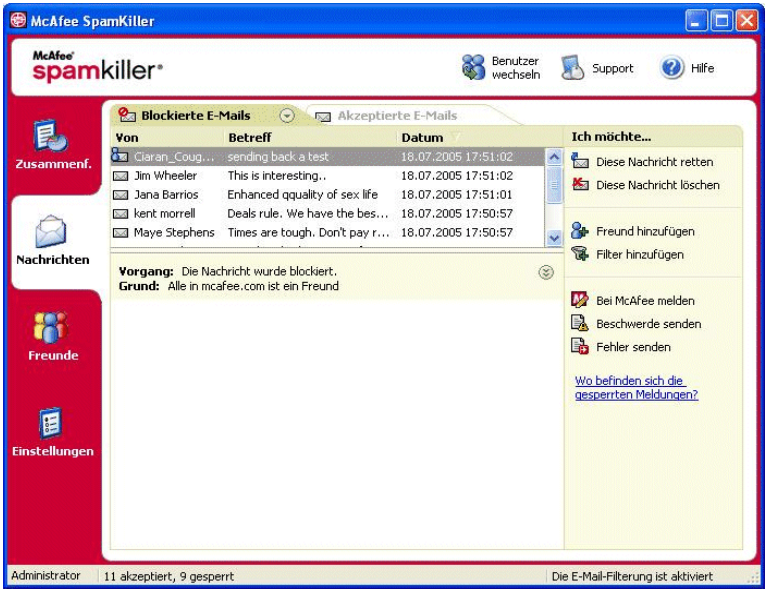


Abbildung 5-14. Seite „Nachrichten“

Registerkarte „Blockierte E-Mails“

Durch Klicken auf die Registerkarte **Blockierte E-Mails** auf der Seite „Nachrichten“ können Sie die von SpamKiller blockierten Nachrichten anzeigen.

> **HINWEIS**
> Sie können die blockierten Nachrichten auch in Microsoft Outlook anzeigen. Klicken Sie dazu im SpamKiller-Menü auf **Blockierte Meldungen anzeigen**.

Blockierte Nachrichten sind die Nachrichten, die von SpamKiller als Spam identifiziert wurden. SpamKiller entfernt diese Nachrichten aus Ihrem Posteingang und verschiebt sie auf die Seite „Blockierte E-Mails“.

Auf der Seite „Blockierte E-Mails“ werden alle Spam-Nachrichten angezeigt, die aus Ihren E-Mail-Konten entfernt wurden. Wenn Sie die blockierten Nachrichten für ein bestimmtes Konto anzeigen möchten, klicken Sie auf der Registerkarte **Blockierte E-Mails** auf den nach unten zeigenden Pfeil , und wählen Sie das Konto aus, das angezeigt werden soll.

Im oberen Bereich der Seite „Nachrichten“ werden die Spam-Nachrichten nach Datum sortiert aufgelistet. Die neueste Nachricht wird zuerst angezeigt. Im unteren Teil wird der Text der ausgewählten Nachricht angezeigt.

> **HINWEIS**
> Wenn Sie Windows 2000 oder Windows XP verwenden, in SpamKiller mehrere Benutzer hinzugefügt und sich bei SpamKiller als Benutzer mit eingeschränkten Rechten angemeldet haben, wird der Inhalt der Nachricht nicht angezeigt.

Der mittlere Fensterbereich enthält nähere Informationen zur Nachricht. Klicken Sie auf die Schaltfläche mit den nach unten zeigenden Pfeilen , um den Fensterbereich mit den Nachrichtendetails zu erweitern und den Nachrichtentext und die Informationen im Nachrichten-Header im nativen Format, einschließlich aller HTML-Formatierungs-Tags, anzuzeigen. Der Bereich mit den Nachrichtendetails enthält folgende Informationen:

- **Aktion**: Beschreibt, wie SpamKiller die Spam-Nachricht behandelt hat. „Aktion“ ist mit der Aktion des Filters verknüpft, der die Nachricht blockiert hat.
- **Grund**: Erläutert, warum die Nachricht von SpamKiller blockiert wurde. Sie können auf den Grund klicken, um den Filter-Editor zu öffnen und den Filter anzuzeigen. Der Filter-Editor zeigt an, wonach der Filter in einer Nachricht sucht und welche Maßnahmen SpamKiller gegen Nachrichten ergreift, die vom Filter als Spam erkannt wurden.
- **Von**: Zeigt den Absender der Nachricht an.
- **Datum**: Zeigt das Sendedatum der Nachricht an.
- **An**: Zeigt den Empfänger der Nachricht an.
- **Betreff**: Gibt das Thema der Nachricht in der Betreffzeile an.

Wenn manuelle Beschwerden oder Fehlermeldungen gesendet wurden, wird in der Spalte am linken Rand für die jeweilige Nachricht eines der folgenden Symbole angezeigt.

- Beschwerde : Gibt an, dass eine Beschwerde über diese Nachricht gesendet wurde.
- Fehlermeldung : Zeigt an, dass an die in der Spam-Nachricht angegebene Antwortadresse eine Fehlermeldung gesendet wurde.
- Beschwerde und Fehlermeldung : Gibt an, dass sowohl eine Beschwerde als auch eine Fehlermeldung gesendet wurde.

Weitere Informationen zu den Speicherorten blockierter Nachrichten finden Sie unter *Speicherort der blockierten Nachrichten* auf Seite 135.

Registerkarte „Akzeptierte E-Mails“

Durch Klicken auf die Registerkarte **Akzeptierte E-Mails** auf der Seite „Nachrichten“ können Sie die von SpamKiller als erwünscht erkannten Nachrichten anzeigen.

Auf der Seite „Akzeptierte E-Mails“ werden alle Nachrichten in den Posteingängen aller Ihrer E-Mail-Konten angezeigt. Bei MAPI-Konten enthält die Seite „Akzeptierte E-Mails“ jedoch keine internen E-Mails. Wenn Sie die akzeptierten Nachrichten für ein bestimmtes Konto anzeigen möchten, klicken Sie auf der Registerkarte **Akzeptierte E-Mails** auf den nach unten zeigenden Pfeil , und wählen Sie das Konto aus, das angezeigt werden soll.

HINWEIS
SpamKiller ist so eingerichtet, dass erwünschte E-Mail-Nachrichten akzeptiert und nicht blockiert werden. Falls jedoch erwünschte E-Mail-Nachrichten in der Liste der blockierte E-Mails angezeigt werden, können Sie diese Nachrichten in den Posteingang (und damit in die Liste der akzeptierten E-Mails) zurückholen, indem Sie sie auswählen und dann auf **Diese Meldung retten** klicken.

Im oberen Bereich der Registerkarte „Akzeptierte E-Mails“ werden die akzeptierten Nachrichten nach Datum sortiert aufgelistet. Im unteren Bereich wird der Text der ausgewählten Nachricht angezeigt.

Im mittleren Bereich finden Sie Informationen dazu, ob die Nachricht von einer Person aus der Freunde-Liste stammt oder die Kriterien eines Filters erfüllt, für den als Aktion entweder **Akzeptieren** oder **Als möglichen Spam markieren** festgelegt wurde. Klicken Sie auf die Schaltfläche mit den nach unten zeigenden Pfeilen , um den Fensterbereich mit den Nachrichtendetails zu erweitern und den Nachrichtentext und die Informationen im Nachrichten-Header im nativen Format, einschließlich aller HTML-Formatierungs-Tags, anzuzeigen..

Der Bereich mit den Nachrichtendetails enthält die folgenden Informationen:

- **Aktion**: Beschreibt, wie SpamKiller die Nachricht behandelt hat.
- **Grund**: Wenn eine Nachricht markiert wurde, wird unter „Grund“ erläutert, warum die Nachricht von SpamKiller markiert wurde.
- **Von**: Zeigt den Absender der Nachricht an.
- **Datum**: Zeigt das Sendedatum der Nachricht an.
- **An**: Zeigt den Empfänger der Nachricht an.
- **Betreff**: Gibt das Thema der Nachricht in der Betreffzeile an.

Neben der Nachricht wird eines der folgenden Symbole angezeigt:

- E-Mail von einem Freund : SpamKiller hat erkannt, dass der Absender der Nachricht in einer der Freunde-Listen eingetragen ist. Diese Nachricht ist eine erwünschte Nachricht.
- Möglicher Spam : Die Nachricht erfüllt die Kriterien eines Filters, für den als Aktion „Als möglichen Spam markieren“ festgelegt wurde.
- Beschwerde : Gibt an, dass eine Beschwerde über diese Nachricht gesendet wurde.
- Fehlermeldung : Gibt an, dass an die in der Spam-Nachricht angegebene Antwortadresse eine Fehlermeldung gesendet wurde.
- Beschwerde und Fehlermeldung : Gibt an, dass sowohl eine Beschwerde als auch eine Fehlermeldung gesendet wurde.

Aufgaben für blockierte und akzeptierte E-Mails

Im rechten Bereich der Registerkarten „Blockierte E-Mails“ und „Akzeptierte E-Mails“ finden Sie eine Liste der Aufgaben, die Sie ausführen können.

- **Diese Meldung blockieren**: Die Nachricht wird aus Ihrem Posteingang entfernt und auf die SpamKiller-Seite „Blockierte E-Mails“ verschoben. (Diese Option wird nur auf der Seite „Akzeptierte E-Mails“ angezeigt.)
- **Diese Meldung retten**: Die Nachricht wird wieder in den Posteingang verschoben (diese Option wird nur auf der Seite „Blockierte E-Mails“ angezeigt), und das Dialogfeld **Wiederherstellungsoptionen** wird geöffnet. Sie können den Absender automatisch zur Freunde-Liste hinzufügen und somit alle Nachrichten von diesem Absender retten.
- **Diese Meldung löschen**: Die ausgewählte Nachricht wird gelöscht.
- **Freund hinzufügen**: Sie können der Freunde-Liste den Namen und die E-Mail-Adresse des Absenders sowie eine Domäne oder eine Mailing-Liste hinzufügen.
- **Filter hinzufügen**: Ermöglicht das Erstellen eines Filters.
- **Bei McAfee melden**: Ermöglicht es Ihnen, McAfee über bestimmte nicht blockierte Spam-Nachrichten in Kenntnis zu setzen, die Sie empfangen haben.
- **Beschwerde senden**: Sendet eine Beschwerde über die Spam-Nachricht an den Administrator der Domäne des Absenders bzw. an eine andere von Ihnen eingegebene E-Mail-Adresse.
- **Fehler senden**: Sendet eine Fehlermeldung an die in der Spam-Nachricht angegebene Antwortadresse.

Wiederherstellen von Nachrichten

Wenn die Seite „Blockierte E-Mails“ oder der SpamKiller-Ordner in Microsoft Outlook und Outlook Express erwünschte E-Mails enthält, können Sie diese Nachrichten in den Posteingang zurückholen:

Über die Registerkarte „Blockierte E-Mails“

1. Klicken Sie auf die Registerkarte **Nachrichten** und dann auf die Registerkarte **Blockierte E-Mails**.

   Oder

   Wählen Sie im SpamKiller-Menü in Microsoft Outlook oder Outlook Express die Option **Blockierte Meldungen anzeigen**, um die Registerkarte „Blockierte E-Mails“ für dieses Konto anzuzeigen.

2. Markieren Sie eine Nachricht, und klicken Sie anschließend auf **Diese Meldung retten** . Das Dialogfeld **Wiederherstellungsoptionen** wird geöffnet.

   - **Freund hinzufügen**: Mit dieser Option können Sie den Absender in die Freunde-Liste aufnehmen.
   - **Alle vom selben Absender wiederherstellen**: Über diese Option können Sie alle blockierten Nachrichten vom Absender der ausgewählten Nachricht wiederherstellen.

3. Klicken Sie auf **OK**. Die Nachricht wird wieder in den Posteingang verschoben und auf der Seite „Akzeptierte E-Mails“ angezeigt.

Über den SpamKiller-Ordner in Microsoft Outlook oder Outlook Express

Markieren Sie die Nachricht(en), und klicken Sie im SpamKiller-Menü oder in der Symbolleiste auf **Auswahl wiederherstellen**. Die ausgewählten Nachrichten werden wieder in den Posteingang verschoben, und die Markierung (standardmäßig [SPAM]) wird entfernt.

Blockieren von Nachrichten

Sie können Spam-Nachrichten, die sich derzeit in Ihrem Posteingang befinden, manuell blockieren. Beim Blockieren einer Nachricht erstellt SpamKiller automatisch einen Filter, mit dem diese Nachricht aus dem Posteingang entfernt wird. Nachrichten im Posteingang können Sie sowohl von der Registerkarte „Akzeptierte E-Mails“ als auch von Microsoft Outlook aus blockieren.

Über die Registerkarte „Akzeptierte E-Mails“

1. Klicken Sie auf die Registerkarte **Nachrichten** und dann auf die Registerkarte **Akzeptierte E-Mails**. Die Seite „Akzeptierte E-Mails“ wird geöffnet, in der die derzeit im Posteingang enthaltenen Nachrichten angezeigt werden.
2. Markieren Sie eine Nachricht, und klicken Sie auf **Diese Meldung blockieren**. Die Nachricht wird aus dem Posteingang und von der Seite „Akzeptierte E-Mails“ entfernt, und auf der Seite „Blockierte E-Mails“ wird eine Kopie der Nachricht angezeigt.

Über Microsoft Outlook

In Microsoft Outlook werden Nachrichten von Benutzern eines Exchange-Servers als sicher eingestuft und somit nicht von SpamKiller gefiltert. Es werden nur Nachrichten von externen Quellen gefiltert.

1. Öffnen Sie Ihren Posteingang in Microsoft Outlook bzw. Outlook Express.
2. Wählen Sie eine Nachricht aus, und klicken Sie anschließend auf . Eine Kopie der Nachricht wird auf der Seite „Blockierte E-Mails“ abgelegt.

Speicherort der blockierten Nachrichten

Standardmäßig werden Spam-Nachrichten als [SPAM] markiert und in den SpamKiller-Ordner in Outlook und Outlook Express oder in Ihrem Posteingang verschoben. Markierte Nachrichten werden auch auf der Seite „Akzeptierte E-Mails“ angezeigt.

Manuelles Löschen von Nachrichten

1. Klicken Sie auf die Registerkarte **Nachrichten** und dann auf die Registerkarte **Blockierte E-Mails**.

   Oder

   Wählen Sie im SpamKiller-Menü in Microsoft Outlook oder Outlook Express die Option **Blockierte Meldungen anzeigen**, um die Registerkarte „Blockierte E-Mails“ für dieses Konto anzuzeigen.
2. Wählen Sie die zu löschende Nachricht aus.
3. Klicken Sie auf **Diese Meldung löschen**. Ein Bestätigungsdialogfeld wird eingeblendet.
4. Klicken Sie auf **Ja**, um die Nachricht zu löschen.

Ändern der Einstellungen, wie Spam-Nachrichten behandelt werden

Erkannte Spam-Nachrichten werden markiert oder blockiert. Bei jeder Verbindungsherstellung mit Ihrem Server werden die Spam-Nachrichten von SpamKiller entfernt.

Markieren mit Tags

Die Betreffzeile der E-Mail wird mit [SPAM] gekennzeichnet, und die Nachricht wird in Microsoft Outlook bzw. Outlook Express in den Posteingang oder SpamKiller-Ordner verschoben.

Blockieren

Die Nachricht wird entfernt und auf die SpamKiller-Seite „Blockierte E-Mails“ verschoben. Wenn erwünschte E-Mails blockiert werden, können Sie diese Nachrichten retten (siehe „Wiederherstellen von Nachrichten“).

Nach Ablauf von 15 Tagen werden die blockierten Nachrichten von SpamKiller automatisch aus der Seite „Blockierte E-Mails“ gelöscht. Sie können die Häufigkeit dieser automatischen Löschvorgänge ändern.

Nachrichten auf der Seite „Akzeptierte E-Mails“ werden von SpamKiller nicht automatisch gelöscht, da diese Seite die gleichen Nachrichten wie Ihr Posteingang enthält.

Ändern der Einstellungen, wie Spam-Nachrichten von SpamKiller behandelt werden

1. Klicken Sie auf die Registerkarte **Einstellungen** und dann auf die Symbolschaltfläche **Filteroptionen**.
2. Klicken Sie auf die Registerkarte **Verarbeitung**.

   - **Spam im Ordner mit blockierten E-Mails speichern**: Die Spam-Nachrichten werden aus Ihrem Posteingang entfernt und auf die SpamKiller-Seite „Blockierte E-Mails“ verschoben.
   - **Spam kennzeichnen und im Posteingang beibehalten**: Dies ist die Standardeinstellung. Die Spam-Nachrichten verbleiben in Ihrem Posteingang, wobei die Betreffzeile der Nachricht mit dem Tag [SPAM] gekennzeichnet wird.

     Blockierte E-Mails beibehalten für ____ Tage: Die blockierten Nachrichten werden für die angegebene Dauer auf der Seite „Blockierte E-Mails“ gespeichert.

Akzeptierte E-Mails aufbewahren für ____ Tage: Die akzeptierten Nachrichten werden für die angegebene Dauer auf der Seite „Akzeptierte E-Mails“ gespeichert.

3 Klicken Sie auf **OK**.

Verwenden des Anti-Phishing-Filters

Unangeforderte E-Mails werden als Spam (E-Mails, in denen Sie zum Kauf aufgefordert werden) oder als Phishing kategorisiert (E-Mails, in denen Sie aufgefordert werden, persönliche Informationen an eine bekannte oder mögliche Betrugs-Website bereitzustellen).

Der McAfee Anti-Phishing-Filter verhindert, dass Sie auf Websites auf der schwarzen Liste (bekannte Phishing- oder ähnliche Websites) bzw. auf Websites auf der grauen Liste (mit gefährlichen Inhalten oder Links zu Websites auf der schwarzen Liste) zugreifen können.

Wenn Sie auf eine bekannte oder mögliche Betrugs-Website zugreifen, werden Sie auf die Seite des McAfee Anti-Phishing-Filters umgeleitet.

So ändern Sie die Anti-Phishing-Einstellungen:

1 Öffnen Sie Internet Explorer.

2 Wählen Sie im Menü **Extras** die Option **McAfee Anti-Phishing-Filter**.

- **Website-Filter aktivieren**: Diese Einstellung ist standardmäßig aktiviert. Zum Deaktivieren des Anti-Phishing-Filters deaktivieren Sie dieses Kontrollkästchen.
- **Zugriff auf Websites auf schwarzer Liste zulassen**: Mit dieser Option wird ein Link auf der Umleitungsseite für Websites auf der schwarzen Liste erstellt. Durch Klicken auf diesen Link wird die Website geöffnet.
- **Zugriff auf Websites auf grauer Liste zulassen**: Mit dieser Option wird ein Link auf der Umleitungsseite für Websites auf der grauen Liste erstellt. Durch Klicken auf diesen Link wird die Website geöffnet.

3 Klicken Sie auf **OK**, wenn Sie den Vorgang abgeschlossen haben.

Hinzufügen von Freunden zu einer Freunde-Liste

Siehe *Hinzufügen von Freunden über die Registerkarte „Blockierte E-Mails“ oder „Akzeptierte E-Mails“* auf Seite 127.

Hinzufügen von Filtern

Ausführliche Informationen zu Filtern finden Sie unter *Arbeiten mit Filtern* in der Online-Hilfe.

1 Zum Erstellen eines allgemeinen Filters klicken Sie auf die Registerkarte **Einstellungen**, wählen Sie **Allgemeine Filter**, und klicken Sie auf **Hinzufügen**.

Oder

Zum Erstellen eines persönlichen Filters klicken Sie auf die Registerkarte **Einstellungen**, wählen Sie **Persönliche Filter**, und klicken Sie auf **Hinzufügen**.

Oder

Klicken Sie auf die Registerkarte **Nachrichten** und dann auf die Registerkarte **Blockierte E-Mails** bzw. **Akzeptierte E-Mails**. Klicken Sie anschließend auf **Filter hinzufügen**.

2 Klicken Sie auf **Hinzufügen**, um eine Filterbedingung zu erstellen. Das Dialogfeld **Filterbedingung** wird angezeigt.

3 Erstellen Sie eine Filterbedingung, indem Sie die folgenden Schritte ausführen.

Eine Filterbedingung ist eine Anweisung an SpamKiller, wonach in den Nachrichten gesucht werden soll. Eine solche Bedingung kann z. B. wie folgt lauten: „Nachrichtentext enthält 'Hypothek'". In diesem Fall sucht der Filter nach Nachrichten, in deren Text das Wort „Hypothek" enthalten ist. Weitere Informationen finden Sie unter *Filterbedingungen* in der Online-Hilfe.

a Wählen Sie im ersten Feld einen Bedingungstyp aus.

b Geben Sie in die anderen Felder Werte ein bzw. wählen Sie Werte aus.

c Wenn die folgenden Optionen angezeigt werden, aktivieren Sie sie wie gewünscht, um die Filterbedingung noch genauer zu definieren.

Auch in Formatierungscodes suchen: Diese Option wird nur angezeigt, wenn laut Filterbedingung der Nachrichtentext durchsucht werden soll. Wenn Sie dieses Kontrollkästchen aktivieren, durchsucht SpamKiller sowohl den Nachrichtentext als auch die Nachrichtenformatierungscodes für den angegebenen Nachrichtentext.

Variationen abgleichen: Ermöglicht es SpamKiller, von Spammern häufig absichtlich falsch verwendete Schreibweisen zu erkennen. Beispielsweise könnte das Wort „Hypothek" auch „Hyp@th3k" geschrieben werden, um von Filtern nicht erkannt zu werden.

Regular Expressions (RegEx): Mit dieser Option können Sie in den Filterbedingungen verwendete Zeichenstrukturen festlegen. Zum Prüfen einer Zeichenstruktur klicken Sie auf **RegEx testen**.

Groß- und Kleinschreibung beachten: Diese Option wird nur bei Bedingungen angezeigt, in denen Sie einen Bedingungswert eingegeben haben. Wenn Sie dieses Kontrollkästchen aktivieren, unterscheidet SpamKiller beim eingegebenen Wert zwischen Groß- und Kleinbuchstaben.

d Klicken Sie auf **OK**.

4 Erstellen Sie eine weitere Filterbedingung, wie im Folgenden beschrieben, oder wechseln Sie zu Schritt 5, um eine Filteraktion auszuwählen.

a Klicken Sie auf **Hinzufügen**, und erstellen Sie dann die Filterbedingung. Klicken Sie nach dem Erstellen der Filterbedingung auf **OK**.

Beide Filterbedingungen werden in der Liste „Filterbedingungen“ angezeigt und sind durch **und** miteinander verbunden. Das **und** bedeutet, dass SpamKiller den Posteingang nach Nachrichten durchsucht, die *beide* Filterbedingungen erfüllen. Wenn SpamKiller nur nach den Nachrichten suchen soll, die lediglich eine der beiden Bedingungen erfüllen, ändern Sie **und** in **oder**, indem Sie auf **und** klicken und dann im angezeigten Feld **oder** wählen.

b Klicken Sie auf **Hinzufügen**, um eine weitere Bedingung zu erstellen, oder wechseln Sie zu Schritt 5, um eine Filteraktion auszuwählen.

Wenn Sie insgesamt drei oder mehr Filterbedingungen erstellt haben, können Sie die Filterbedingungen zu Gruppen zusammenfassen und so Klauseln erstellen. Beispiele für gruppierte Filterbedingungen finden Sie unter *Gruppieren von Filtern* in der Online-Hilfe.

Wenn Sie Filterbedingungen gruppieren möchten, wählen Sie eine Filterbedingung aus, und klicken Sie dann auf **Gruppe**. Um die Gruppierung von Filterbedingungen aufzuheben, wählen Sie die entsprechende Gruppe aus und klicken Sie dann auf **Gruppierung aufheben**.

5 Wählen Sie im Feld **Aktion** eine Filteraktion aus. Die Filteraktion weist SpamKiller an, wie mit den durch diesen Filter gefundenen Nachrichten verfahren werden soll. Weitere Informationen finden Sie unter *Filteraktionen* in der Online-Hilfe.

6 Klicken Sie auf **Erweitert**, um erweiterte Filteroptionen auszuwählen. (Das Auswählen erweiterter Optionen ist optional.) Weitere Informationen finden Sie unter *Erweiterte Filteroptionen* in der Online-Hilfe.

7 Klicken Sie nach dem Erstellen des Filters auf **OK**.

HINWEIS
Wenn Sie eine Bedingung bearbeiten möchten, wählen Sie sie aus, und klicken Sie dann auf **Bearbeiten**. Um eine Bedingung zu löschen, wählen Sie sie aus, und klicken Sie dann auf **Löschen**.

Regelmäßige Ausdrücke

Regelmäßige Ausdrücke sind nur für die folgenden Filterbedingungen verfügbar: **Betreff**, **Meldungstext**, **Mindestens einer der folgenden Sätze**.

Diese Sonderzeichen und Folgen können bei der Definition von Filterbedingungen als regelmäßige Ausdrücke verwendet werden. Beispiel:

- Der regelmäßige Ausdruck **[0-9]*\.[0-9]+** entspricht Gleitkommazahlen, die eine nicht technische Schreibweise angeben. Der regelmäßige Ausdruck entspricht „12.12“, „.1212“ und „12.0“, nicht jedoch „12“ und „12“.
- Der regelmäßige Ausdruck **\D*[0-9]+\D*** entspricht allen Wörtern mit Zahlen, z. B. „SpamKi11er“ und „V1AGRA“, nicht jedoch „SpamKiller“ und „VIAGRA“.

****

Kennzeichnet das nächste Zeichen entweder als Sonderzeichen oder als Buchstaben. Beispielsweise steht „n“ für das Zeichen „n“. „\n“ entspricht einem Zeilenvorschubzeichen Die Folge „\\“ entspricht „\“, und „\(“ entspricht „(“.

^

Kennzeichnet den Beginn einer Eingabe.

$

Kennzeichnet das Ende einer Eingabe.

*****

Entspricht dem vorhergehenden Zeichen keinmal oder mehrmals. Zum Beispiel entspricht „zo*“ entweder „z“ oder „zoo“.

+

Entspricht dem vorhergehenden Zeichen einmal oder mehrmals. Zum Beispiel entspricht „zo+“ „zoo“, nicht jedoch „z“.

?

Entspricht dem vorhergehenden Zeichen keinmal oder einmal. Beispielsweise steht „a?ch?“ für das „ch“ in „nicht“.

.

Entspricht einem beliebigen Einzelzeichen, außer einem Zeilenvorschubzeichen.

(pattern)

Entspricht dem Muster (englisch Pattern) und speichert den übereinstimmenden Wert. Die entsprechende Teilzeichenfolge kann mit Hilfe des Elements „[0]...[n]“ aus der resultierenden Übereinstimmungssammlung abgerufen werden. Zum Angleichen der Klammerzeichen ( ) verwenden Sie „\(“ oder „\)“.

x|y

Entspricht entweder „x“ oder „y“. Zum Beispiel entspricht „z|boot“ „z“ oder „boot“. „(z|b)oo“ steht für „zoo“ oder „boot“.

{n}

Das Zeichen „n“ ist eine positive Ganzzahl und entspricht genau n-Mal. Beispielsweise entspricht „u{2}“ nicht dem „u“ in „Ruth,“, entspricht aber den ersten beiden „u“ in „suuuuuuper“.

{n,}

Das Zeichen „n“ ist eine positive Ganzzahl und entspricht mindestens n-Mal. Beispielsweise stimmt „u{2,}“ nicht mit dem „u“ in „Ruth“ überein und entspricht allen Zeichen „u“ in „suuuuuuper“. Der Ausdruck „u{1,}“ entspricht „u+“. „u{0,}“ entspricht „o*“.

{n,m}

Die Zeichen „m“ und „n“ sind positive Ganzzahlen und entsprechen mindestens n-Mal und höchstens m-Mal. Beispielsweise steht „u{1,3}“ für die ersten drei „u“ in „suuuuuuper“. Der Ausdruck „u{0,1}“ entspricht „u?“.

[xyz]

Ein Zeichensatz. Entspricht einem beliebigen der eingeschlossenen Zeichen. Beispielsweise entspricht „[abc]“ dem „a“ in „ganz“.

[^xyz]

Ein negativer Zeichensatz. Entspricht einem der nicht eingeschlossenen Zeichen. Zum Beispiel entspricht „[^abc]“ dem Buchstaben „g“ im Wort „ganz“.

[a-z]

Eine Zeichenbereich. Entspricht einem beliebigen Zeichen im angegebenen Bereich. Zum Beispiel entspricht „[a-z]“ einem beliebigen Buchstaben in Kleinschreibung aus dem Bereich „a“ bis „z“.

[^m-z]

Ein negativer Zeichenbereich. Entspricht einem beliebigen Zeichen, das nicht im angegebenen Bereich enthalten ist. Zum Beispiel entspricht „[m-z]“ einem beliebigen Buchstaben, der nicht im Bereich „m“ bis „z“ enthalten ist.

\b

Entspricht einer Wortgrenze, d. h. der Position zwischen einem Wort und einem Leerzeichen. Beispielsweise entspricht „ht\b“ dem „ht“ in „nicht“, aber nicht dem „ht“ in „leuchter“.

\B

Entspricht einer Nicht-Wortgrenze. Beispielsweise entspricht „fr*o\B“ dem „fro“ in „immer froh“.

\d

Entspricht einer Ziffer, d. h. [0-9].

\D

Entspricht einem Zeichen, das keine Ziffer ist, d. h. [^0-9].

\f

Entspricht einem Seitenvorschubzeichen.

\n

Entspricht einem Zeilenvorschubzeichen.

\r

Entspricht einem Zeilenumbruchzeichen.

\s

Entspricht beliebigen Leerzeichen, einschließlich Leerzeichen, Tabulator, Seitenvorschub usw. Entspricht „[\f\n\r\t\v]“.

\S

Entspricht einem beliebigen Zeichen, das kein Leerzeichen ist. Entspricht „[^ \f\n\r\t\v]“.

\t

Entspricht einem Tabulatorzeichen.

\v

Entspricht einem vertikalen Tabulatorzeichen.

\w

Entspricht Buchstaben und Ziffern, einschließlich Unterstrich. Entspricht „[A-Za-z0-9_]“.

\W

Entspricht einem Zeichen, das kein Buchstabe oder Ziffer ist. Entspricht „[^A-Za-z0-9_]“.

\num

Entspricht „num“, wobei es sich bei „num“ um eine positive Ganzzahl handelt. Eine Referenz auf gespeicherte übereinstimmende Werte. Zum Beispiel entspricht „(.)\1“ zwei aufeinander folgenden, identischen Zeichen.

\n

Entspricht „n“, wobei es sich bei „n“ um einen oktalen Escape-Wert handelt. Oktale Escape-Werte müssen 1, 2 oder 3 Ziffern lang sein. Zum Beispiel entsprechen „\11“ und „\011“ beide einem Tabulatorzeichen. „\0011“ ist das Äquivalent zu „\001“ und „1“. Oktale Escape-Werte dürfen nicht länger als 256 Zeichen sein. Andernfalls enthalten nur die ersten zwei Ziffern den Ausdruck. Ermöglicht die Verwendung von ASCII-Codes in regelmäßigen Ausdrücken.

\xn

Entspricht „n“, wobei es sich bei „n“ um einen hexadezimalen Escape-Wert handelt. Hexadezimale Escape-Werte müssen genau 2 Ziffern lang sein. Beispielsweise ist „\x41“ die Entsprechung für den Buchstaben „A“. Der Ausdruck „\x041“ entspricht „\x04“ und „1“. Ermöglicht die Verwendung von ASCII-Codes in regelmäßigen Ausdrücken.

Melden von Spam-Nachrichten an McAfee

Sie können Spam-Nachrichten an McAfee senden, wo diese analysiert werden, um entsprechende Filter-Updates zu erstellen.

1. Klicken Sie auf die Registerkarte **Nachrichten** und dann auf die Registerkarte **Blockierte E-Mails** bzw. **Akzeptierte E-Mails**. Die Registerkarte „Blockierte E-Mails“ bzw. „Akzeptierte E-Mails“ wird geöffnet.
2. Wählen Sie eine Nachricht aus, und klicken Sie dann auf **Bei McAfee melden**. Ein Bestätigungsdialogfeld wird eingeblendet.
3. Klicken Sie auf **Ja**. Die Nachricht wird automatisch an McAfee gesendet.

Manuelles Senden von Beschwerden

Sie können dem Absender von Spam-Nachrichten eine Beschwerde senden, um ihn davon abzuhalten, Ihnen weitere Spam-Nachrichten zu senden. Weitere Informationen zum Senden von Beschwerden finden Sie unter *Senden von Beschwerden und Fehlermeldungen* in der Online-Hilfe.

1. Klicken Sie auf die Registerkarte **Nachrichten** und dann auf die Registerkarte **Blockierte E-Mails** bzw. **Akzeptierte E-Mails**. Eine Liste der Nachrichten wird angezeigt.

2 Wählen Sie die Nachricht aus, über die Sie sich beschweren möchten, und klicken Sie dann auf **Beschwerde senden**. Das Dialogfeld **Beschwerde senden** wird geöffnet.

3 Wählen Sie die Person aus, der Sie die Beschwerde senden möchten.

> **WARNUNG**
> Sie sollten jedoch nicht **Absender** wählen, da der Absender durch den Empfang einer Beschwerde erfährt, dass Ihre E-Mail-Adresse gültig ist, was dazu führen kann, dass er Ihnen noch mehr Spam-Nachrichten sendet.

4 Klicken Sie auf **Weiter**, und befolgen Sie die angezeigten Anweisungen.

Senden von Fehlermeldungen

Weitere Informationen zum Senden von Fehlermeldungen finden Sie unter *Senden von Beschwerden und Fehlermeldungen* in der Online-Hilfe.

Sie können festlegen, dass SpamKiller eine Fehlermeldung sendet, um den Absender davon abzuhalten, Ihnen weitere Spam-Nachrichten zu senden.

Manuelles Senden von Fehlermeldungen

1 Klicken Sie auf die Registerkarte **Nachrichten** und dann auf die Registerkarte **Blockierte E-Mails** bzw. **Akzeptierte E-Mails**. Eine Liste der Nachrichten wird angezeigt.

2 Wenn Sie eine Fehlermeldung zu einer bestimmten Spam-Nachricht versenden möchten, wählen Sie die Nachricht aus, und klicken Sie dann auf **Fehler senden**. Daraufhin wird an die in der Spam-Nachricht angegebene Antwortadresse eine Fehlermeldung gesendet.

Index

A

ActiveShield
- aktivieren, 19
- anhalten, 21
- ausschließliches Prüfen von Programmdateien und Dokumenten, 27
- deaktivieren, 19
- Prüfen aller Dateien, 26
- Prüfen aller Dateitypen, 26
- Prüfen auf möglicherweise unerwünschte Programme (PUPs), 29
- Prüfen auf neue, unbekannte Viren, 27
- Prüfen auf Skripts, 27
- prüfen auf Würmer, 23
- Prüfen von Anlagen eingehender Instant Messages, 25
- Prüfen von E-Mails und Anlagen, 21
- Prüfoptionen, 20
- standardmäßige Scan-Einstellung, 21, 24 to 29
- starten, 21
- testen, 16
- Virus bereinigen, 30

Administrator, 87, 119, 121
- Wiederbeschaffen des Kennworts, 88

aktualisieren
- einer Rettungsdiskette, 45
- VirusScan
  - automatisch, 48
  - manuell, 48

Akzeptierte E-Mails
- Aufgaben, 133
- Fehlermeldungen senden, 144
- Freunde zu einer Freunde-Liste hinzufügen, 137
- mit akzeptierten Nachrichten arbeiten, 130
- Symbole in der Liste der akzeptierten Nachrichten, 133

Akzeptierte E-Mails (Registerkarte), 132

Alle Dateien überprüfen, Option (Scan), 35

Anlagen eingehender Instant Messages
- automatisch bereinigen, 25
- Prüfung, 25

Anmelden bei SpamKiller auf einem Computer mit mehreren Benutzern, 122

Anti-Phishing-Filter, verwenden, 137

Anzeigen von Ereignissen im Ereignisprotokoll, 68

Auf möglicherweise unerwünschte Programme überprüfen, Option (Scan), 36

Aufgaben für blockierte und akzeptierte Nachrichten, 133

Automatische Windows-Updates, 78

AVERT, Übermitteln verdächtiger Dateien, 43

B

Bearbeiten von Benutzern, 92
- Altersgruppe, 94
- Benutzerinformationen, 92
- Blockieren von Cookies, 93
- Entfernen von Benutzern, 95
- Internetzugriffszeiten, 94
- Kennwort, 92
- Startbenutzer, 95

Benutzer, 111
- bei SpamKiller anmelden, 122
- Benutzer hinzufügen, 119
- Benutzerprofile bearbeiten, 121
- Benutzerprofile löschen, 122
- Benutzertypen, 119
- Kennwörter erstellen, 120
- Wechseln zwischen Benutzern, 122

Benutzer hinzufügen, 90
- Blockieren von Cookies, 91
- Inhaltsblockade, 90
- Internetzugriffszeiten, 91

Benutzer wechseln (Symbol), 108

Benutzeroptionen, 103
Ablehnen von Cookies, 105
Akzeptieren von Cookies, 104
Ändern Ihres Benutzernamens, 103
Ändern Ihres Kennworts, 103
Leeren des Cache, 104
Blockieren von Nachrichten, 134
Blockierte E-Mails
Aufgaben, 133
Einstellungen ändern, wie Spam-Nachrichten behandelt werden, 136
Fehlermeldungen senden, 144
Freunde zu einer Freunde-Liste hinzufügen, 137
mit blockierten Nachrichten arbeiten, 130
Nachrichten wiederherstellen, 134
Speicherort der blockierten Nachrichten, 135
Symbole in der Liste der blockierten Nachrichten, 131
Blockierte E-Mails (Registerkarte), 130

D

Deinstallation
anderer Firewalls, 53
Dienstprogramme, 100

E

Einrichten des Schreibschutzes für eine Rettungsdiskette, 44
Einrichten von E-Mail-Clients für die Verwendung von SpamKiller, 112
E-Mail-Konten, 111
bearbeiten, 113
Einrichten von E-Mail-Clients für die Verwendung von SpamKiller, 112
hinzufügen, 111
löschen, 112
MAPI-Konten bearbeiten, 117
MSN/Hotmail-Konten bearbeiten, 115
POP3-Konten bearbeiten, 113
E-Mails und Anlagen
automatisch bereinigen
aktivieren, 21
Prüfung
aktivieren, 21
deaktivieren, 23
Fehler, 22
Ereignisprotokoll, 98
anzeigen, 75
Info, 65
verwalten, 75
Ereignisse
anzeigen
alle, 69
aus dieser Woche, 69
bestimmter Tag, 70
mit identischen Ereignisinformationen, 70
von bestimmter Adresse, 70
von heute, 69
Archivieren des Ereignisprotokolls, 75
exportieren, 76
Info, 65
kopieren, 76
Loopback, 67
löschen, 76
Löschen des Ereignisprotokollinhalts, 76
melden, 71
Ratschläge von HackerWatch.org, 71
reagieren auf, 71
verfolgen
Anzeigen von archivierten Ereignisprotokollen, 75
Erläuterung, 65
von 0.0.0.0, 66
von 127.0.0.1, 67
von Computern in Ihrem lokalen Netzwerk (LAN), 67
von privaten IP-Adressen, 68
weitere Informationen, 71
Erstellen einer Rettungsdiskette, 43

F

Filter
aktivieren, 109
deaktivieren, 109
Filter, hinzufügen, 138

Freunde-Liste, 123
Adressbuch importieren, 124
E-Mail-Adresse hinzufügen, 127
Freunde aus der Registerkarte „Blockierte E-Mails“ oder „Akzeptierte E-Mails“ hinzufügen, 127
Funktionen, 87, 107

H

HackerWatch.org
anmelden, 72
Ereignismeldung an, 71
Ratschläge, 71
Hilfe (Symbol), 109
Hinzufügen von E-Mail-Adressen zu einer Freunde-Liste, 127
Hinzufügen von E-Mail-Konten, 111
Hinzufügen von Filtern, 138

I

Importieren von Adressbüchern in eine Freunde-Liste, 124
in Liste der vertrauenswürdigen Programme aufnehmen
PUPs, 32
Internetanwendungen
Ändern von Anwendungsregeln, 64
Info, 63
Zulassen und Blockieren, 64
IP-Adressen
Info, 66
Sperren, 73
vertrauenswürdig, 72

K

Kennwörter, 120
Kinderschutz, 120
Komprimierte Dateien überprüfen, Option (Scan), 35
Konfigurieren
VirusScan
ActiveShield, 18
Scan, 33

L

Liste der erkannten Dateien (Scan), 37, 40
Liste der vertrauenswürdigen Programme bearbeiten, 33
Liste der vertrauenswürdigen PUPs, 33

M

McAfee Privacy Service, 89
Aktualisieren, 90
Anmelden, 89
deaktivieren, 89
Öffnen, 89
McAfee SecurityCenter, 13
Melden von Ereignissen, 71
Melden von Spam-Nachrichten an McAfee, 143
Microsoft Outlook, 38
Möglicherweise unerwünschte Programme (PUPs), 29
bereinigen, 41
entfernen, 32
erkennen, 40
löschen, 41
unter Quarantäne stellen, 41
vertrauenswürdig, 32
Warnungen, 32

N

Nach neuen, unbekannten Viren scannen, Option (Scan), 35
Nachrichten wiederherstellen, 134
Neue Funktionen, 15, 51

O

Optionen, 95
Blockieren von Informationen, 96
Blockieren von Websites, 95
Blockieren von Werbung, 97
Sicherung, 101
Web-Bugs, 97
Zulassen von Cookies, 98
Zulassen von Websites, 96

P

Personal Firewall
testen, 57
Planen von Prüfungen, 38
Prüfoptionen
ActiveShield, 20, 26 to 27
Scan, 33
Prüfung
alle Dateien, 26, 35
auf möglicherweise unerwünschte Programme (PUPs), 29
auf neue, unbekannte Viren, 35
auf Skripts, 27
auf Würmer, 23
komprimierte Dateien, 35
nur Programmdateien und Dokumente, 27
Planen automatischer Prüfungen, 38
über die Microsoft Outlook-Symbolleiste, 38
über Windows-Explorer, 37
Unterordner, 34

Q

Quarantäne
Bereinigen von Dateien, 41 to 42
Hinzufügen von verdächtigen Dateien, 41
Löschen von Dateien, 41
Löschen von verdächtigen Dateien, 42
Übermitteln verdächtiger Dateien, 43
Verwalten von verdächtigen Dateien, 41
Wiederherstellen von bereinigten Dateien, 41 to 42

R

Regelmäßige Ausdrücke, 140
Rettungsdiskette
aktualisieren, 45
Einrichten des Schreibschutzes, 44
erstellen, 43
verwenden, 41, 45

S

Scan
Alle Dateien überprüfen, Option, 35
Auf möglicherweise unerwünschte Programme überprüfen, Option, 36
automatisches Prüfen, 38
Bereinigen eines Virus oder eines möglicherweise unerwünschten Programms, 41
Komprimierte Dateien überprüfen, Option, 35
Löschen eines Virus oder eines möglicherweise unerwünschten Programms, 41
manuelles Prüfen, 33
manuelles Prüfen über die Microsoft Outlook-Symbolleiste, 38
manuelles Prüfen über Windows-Explorer, 38
Nach neuen, unbekannten Viren scannen, Option, 35
Quarantäne für einen Virus oder ein möglicherweise unerwünschtes Programm, 41
testen, 17 to 18
Unterordner überprüfen, Option, 34
Schnellreferenz, iii
ScriptStopper, 27
Seite „Einstellungen“, 111
Seite „Freunde“, 124
Seite „Nachrichten“, 130
Seite „Zusammenfassung“, 110
Setup-Assistent, 88
Shredder, 100
Skripts
anhalten, 31
Warnungen, 31
zulassen, 31
SpamKiller
Akzeptierte E-Mails (Registerkarte), 132
Blockierte E-Mails (Registerkarte), 130
Filter aktivieren, 109
Filter deaktivieren, 109
Standard-Firewall, festlegen, 53
Startbenutzer, 89 to 90

T

Technischer Support, 41
Testen von Personal Firewall, 57
Testen von VirusScan, 16
Trojaner
  erkennen, 40
  Warnungen, 30

U

Übermitteln verdächtiger Dateien an AVERT, 43
Unterordner überprüfen, Option (Scan), 34
Unterstützung (Symbol), 109
Update-Assistent, 20

V

Verfolgen eines Ereignisses, 71
Vertrauenswürdige Programme, 33
Verwenden einer Rettungsdiskette, 45
Viren
  Anhalten potentieller Würmer, 32
  Anhalten verdächtiger Skripts, 31
  automatisches Melden, 45 to 46
  bereinigen, 30, 40
  Entfernen von PUPs, 32
  erkennen, 40
  Erkennung mit ActiveShield, 30
  löschen, 30, 40
  Löschen infizierter Dateien, 31
  Quarantäne für infizierte Dateien, 31
  unter Quarantäne stellen, 30, 40
  Warnungen, 30
  Zulassen verdächtiger Skripts, 31
VirusScan
  automatisches Aktualisieren, 48
  automatisches Melden von Viren, 45 to 46
  manuelles Aktualisieren, 48
  Planen von Prüfungen, 38
  Prüfen über die Microsoft Outlook-Symbolleiste, 38
  Prüfen über Windows-Explorer, 38
  testen, 16

W

Warnungen
  Anwendung fordert Internetzugriff an, 77
  Anwendung fordert Serverzugriff an, 77
  bei infizierten Dateien, 30
  bei infizierten E-Mails, 31
  bei potentiellen Würmern, 32
  bei PUPs, 32
  bei verdächtigen Skripts, 31
  bei Viren, 30
  Die Anwendung wurde geändert, 77
  Internetanwendung blockiert, 77
  Neu zugelassene Anwendung, 83
  Versuch, eine Verbindung herzustellen, wurde blockiert, 84
Wechseln zwischen Benutzern, 122
Windows-Explorer, 38
Windows-Firewall, 53
World Virus Map
  anzeigen, 46
  melden, 45
WormStopper, 23
Würmer
  anhalten, 32
  erkennen, 30, 40
  Warnungen, 30, 32

Z

Zusammenfassung, 57